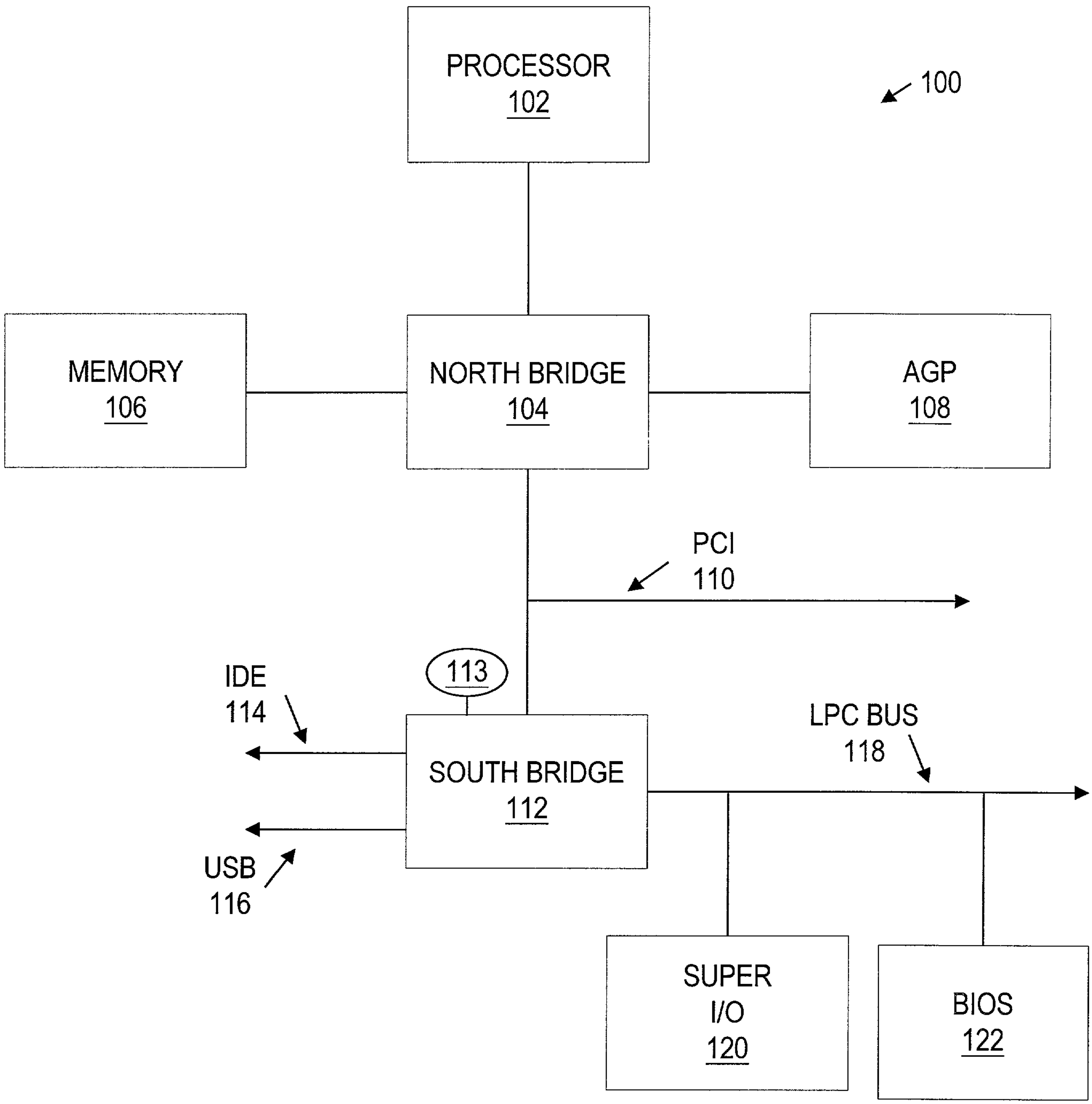

Fig. 1A
(Prior Art)

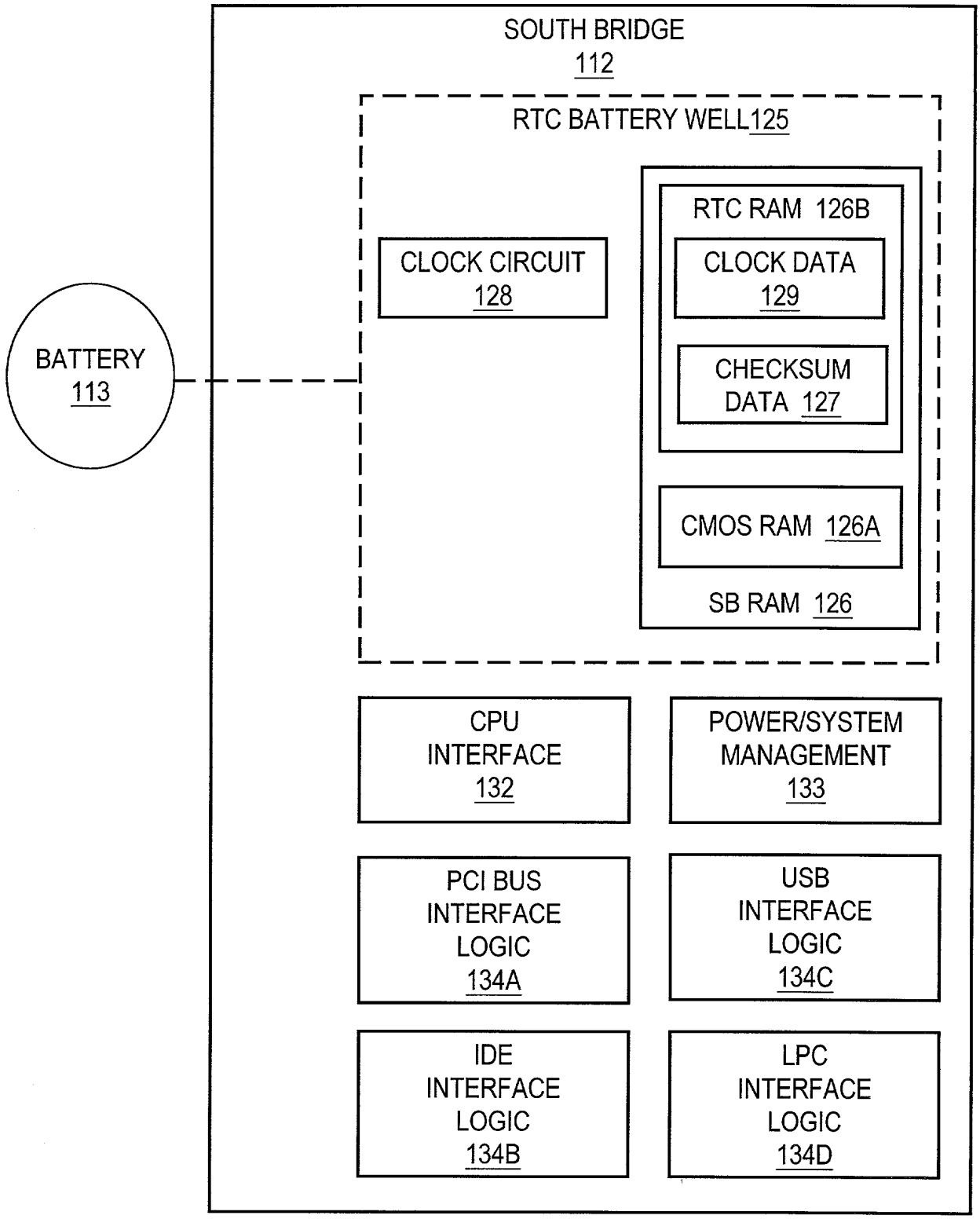

Fig. 1B
(Prior Art)

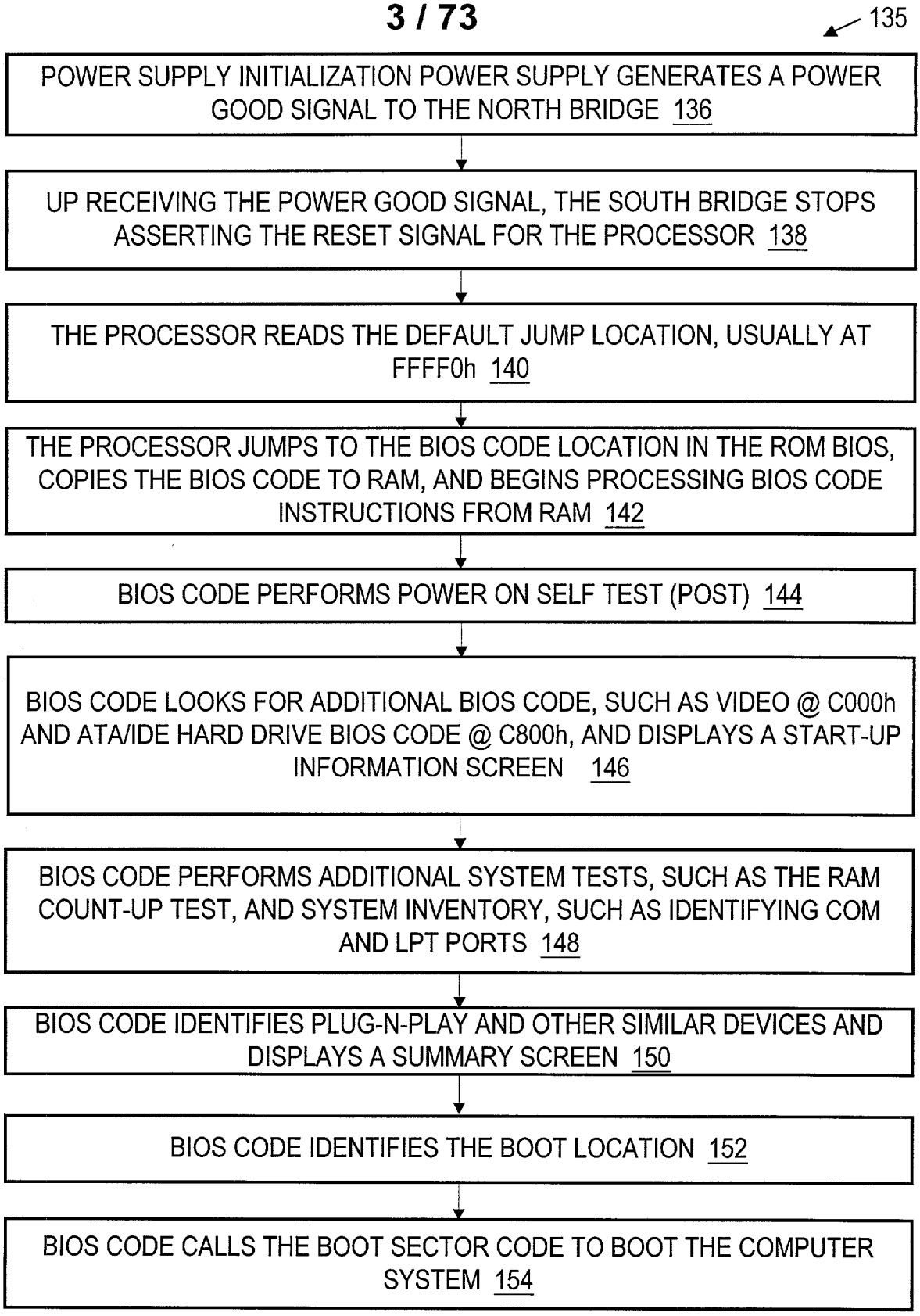

Fig. 2A
(Prior Art)

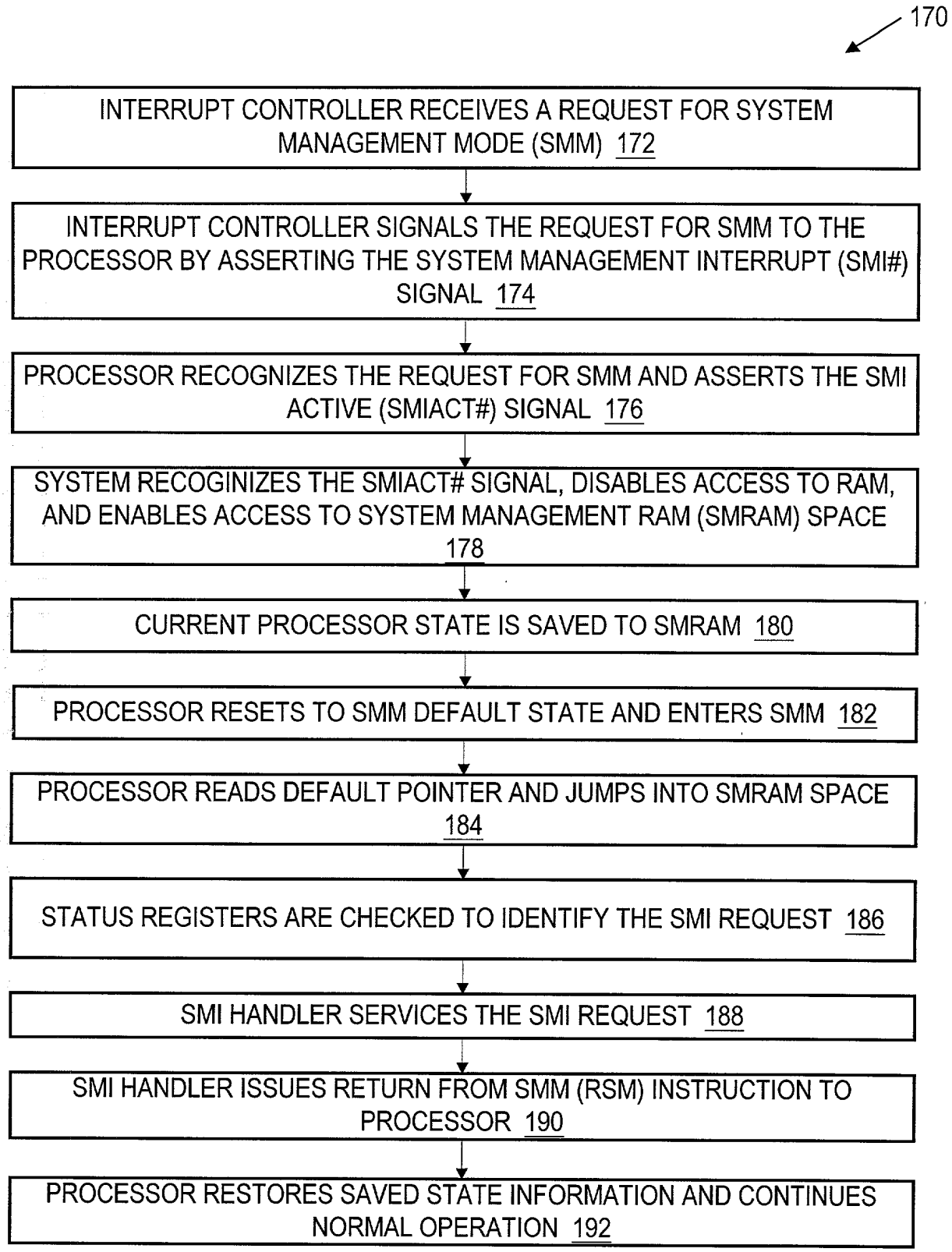

Fig. 2B
(Prior Art)

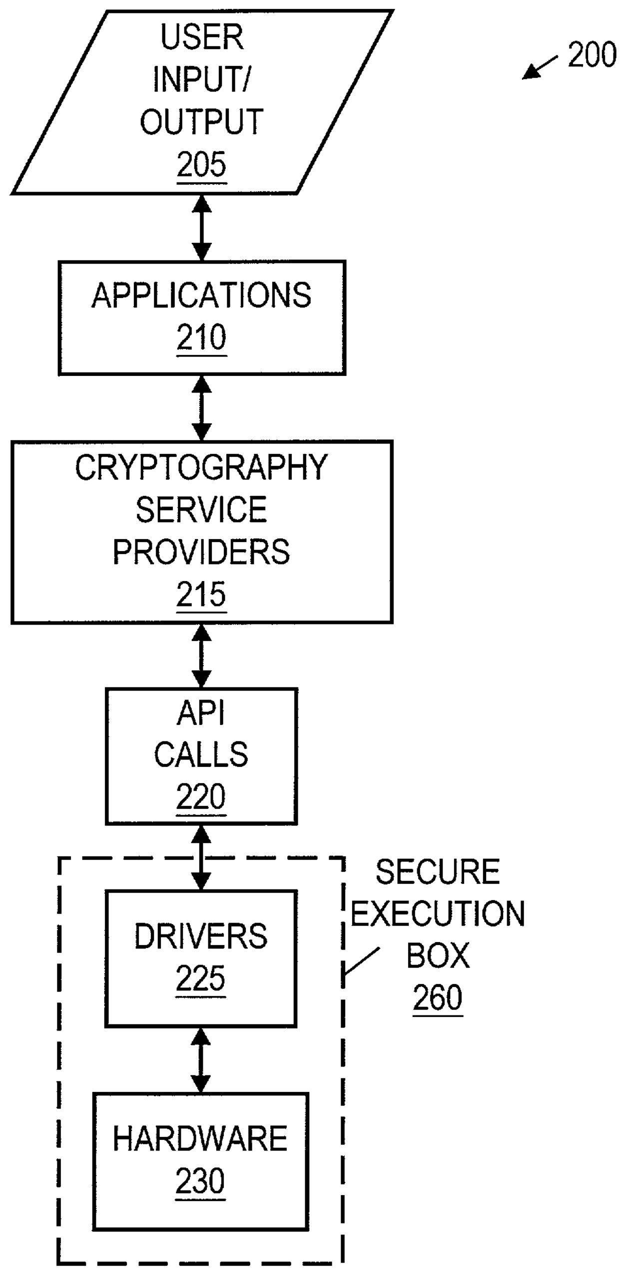

Fig. 3

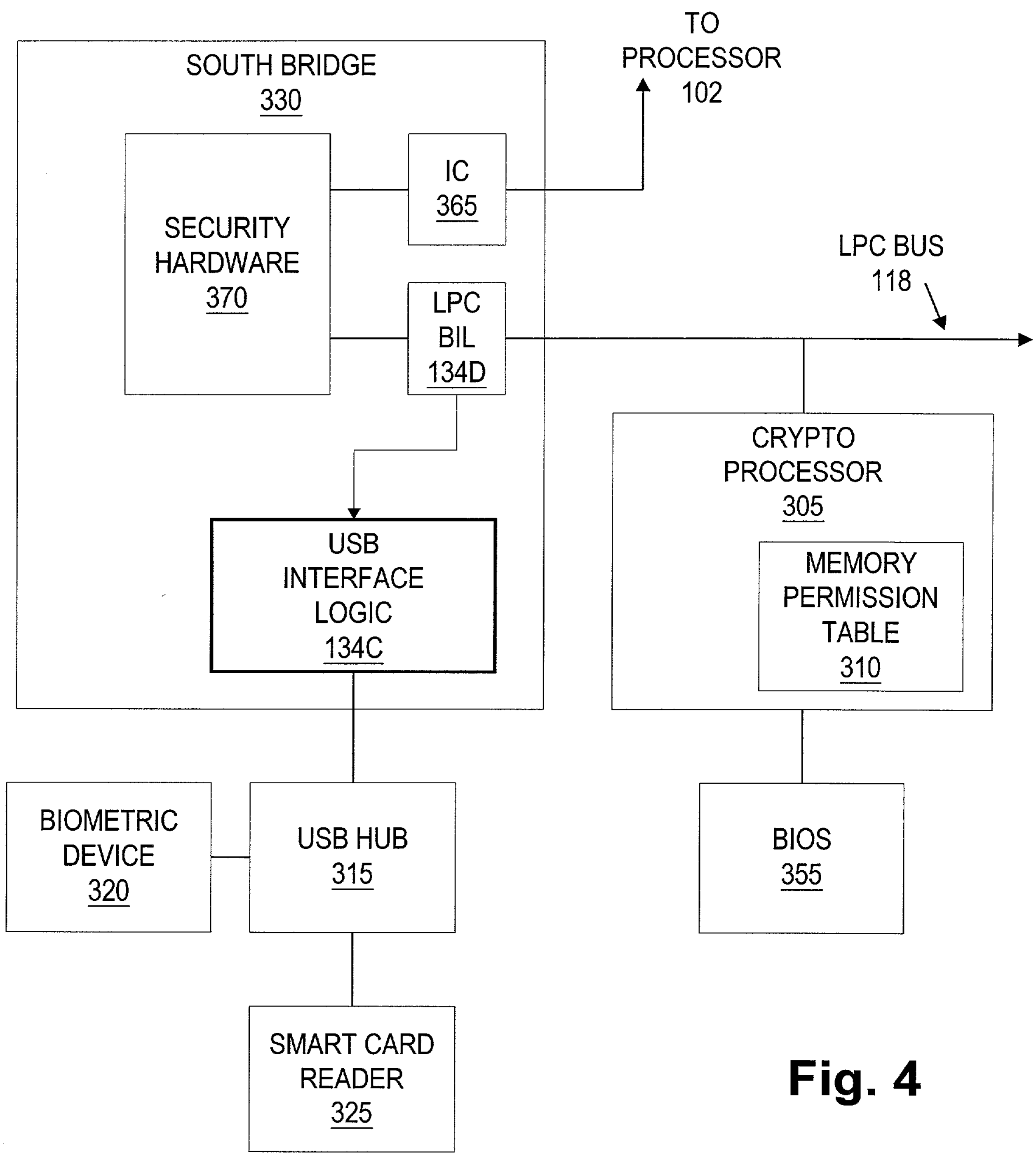
SOUTH BRIDGE
330
SECURITY
HARDWARE
370
IC
365
TO
PROCESSOR
102
LPC
BIL
134D
LPC BUS
118
USB
INTERFACE
LOGIC
134C
CRYPTO
PROCESSOR
305
MEMORY
PERMISSION
TABLE
310
BIOMETRIC
DEVICE
320
USB HUB
315
BIOS
355
SMART CARD
READER
325

Fig. 4

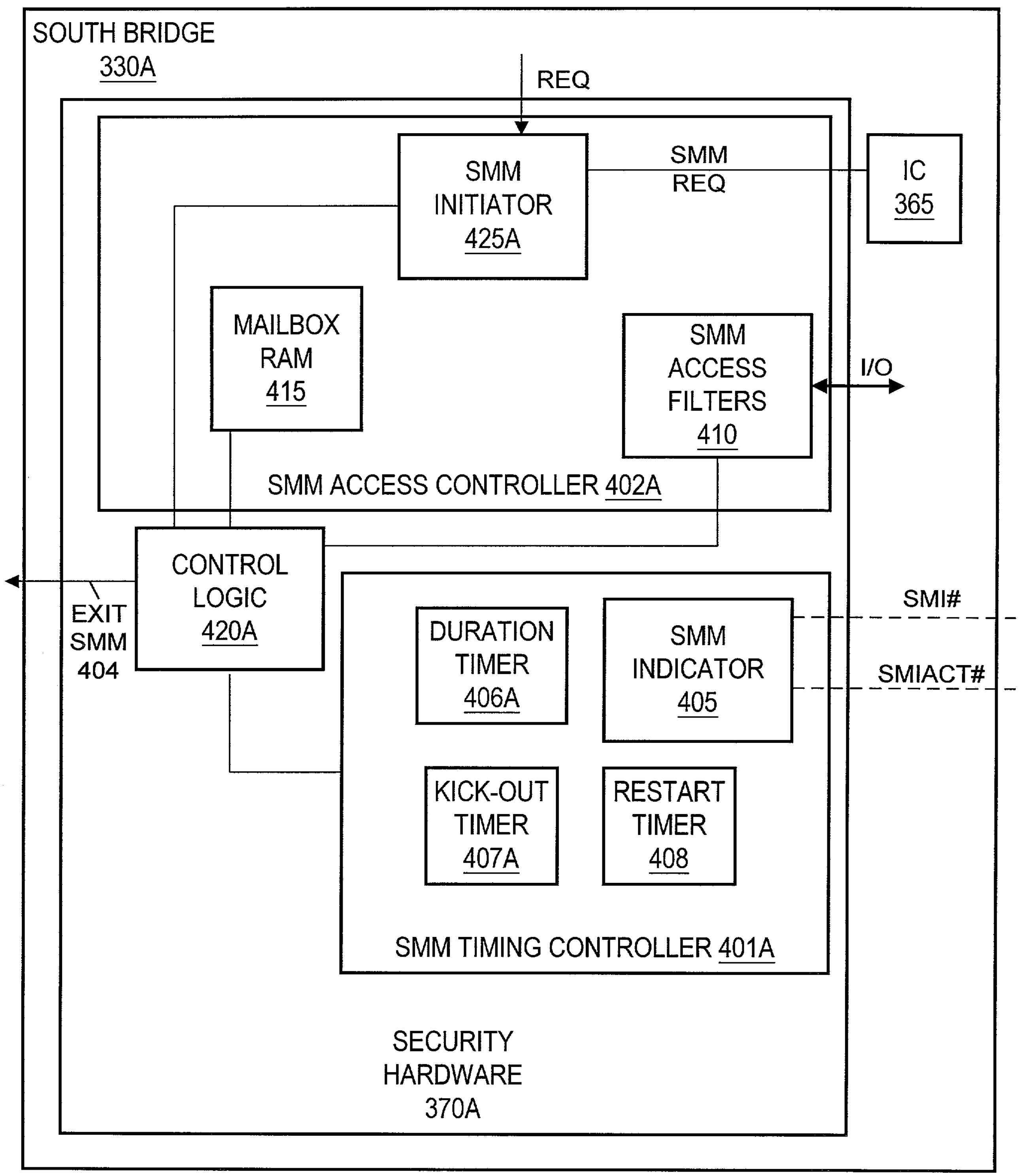
SOUTH BRIDGE
330A
REQ
SMM
INITIATOR
425A
SMM
REQ
IC
365
MAILBOX
RAM
415
SMM
ACCESS
FILTERS
410
I/O
SMM ACCESS CONTROLLER 402A
CONTROL
LOGIC
420A
EXIT
SMM
404
DURATION
TIMER
406A
SMM
INDICATOR
405
SMI#
SMIACT#
KICK-OUT
TIMER
407A
RESTART
TIMER
408
SMM TIMING CONTROLLER 401A
SECURITY
HARDWARE
370A

Fig. 5A

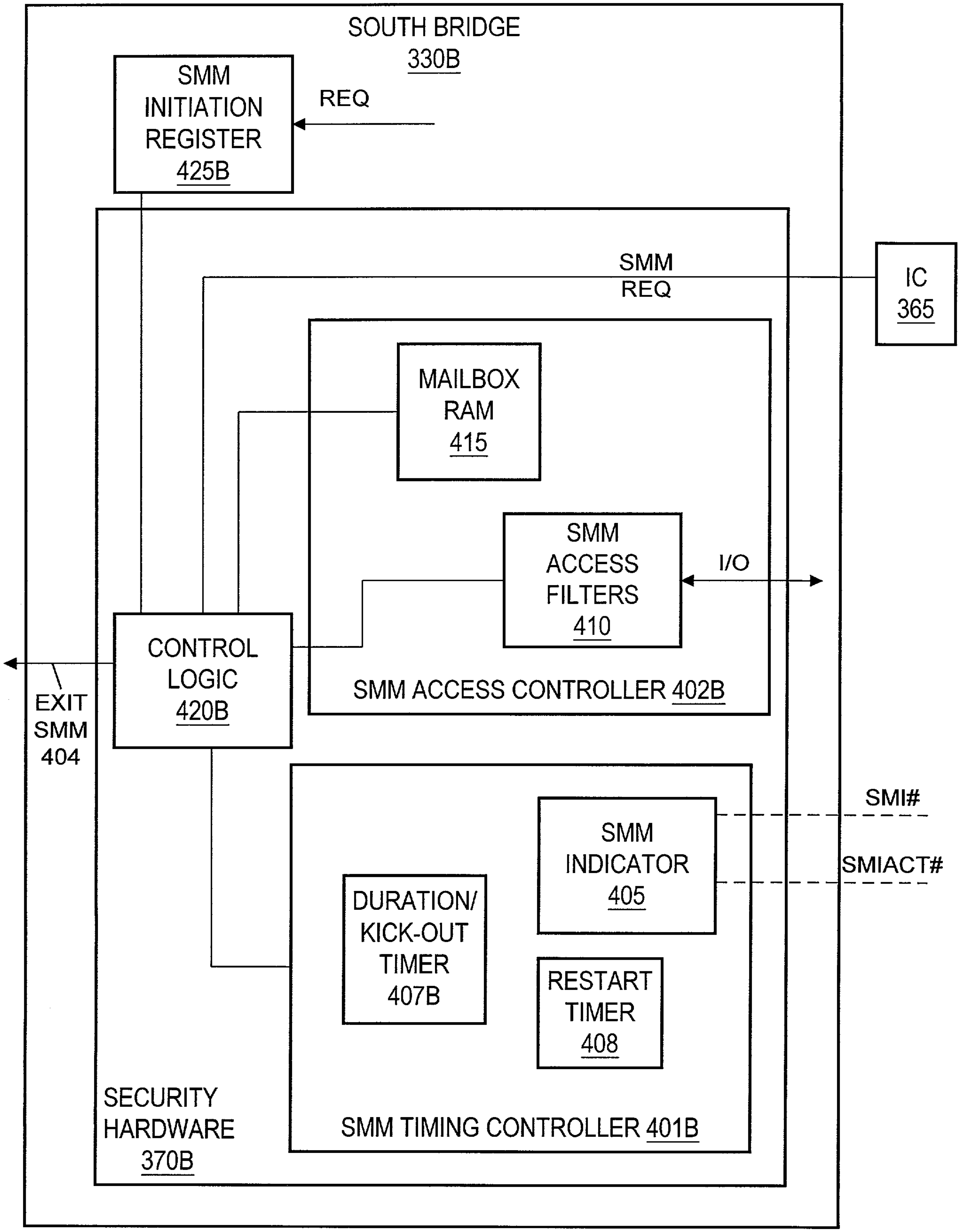

Fig. 5B

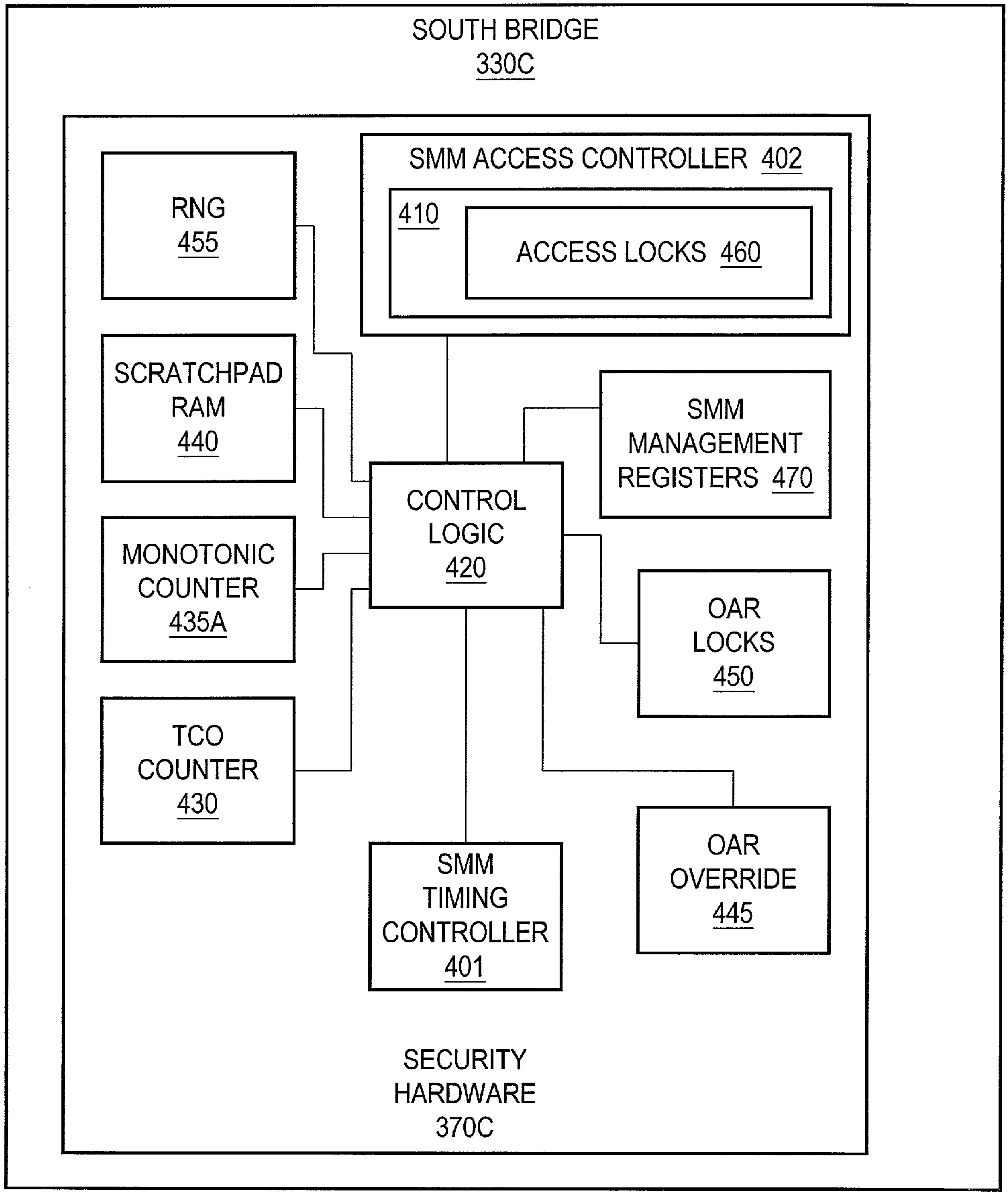

Fig. 6

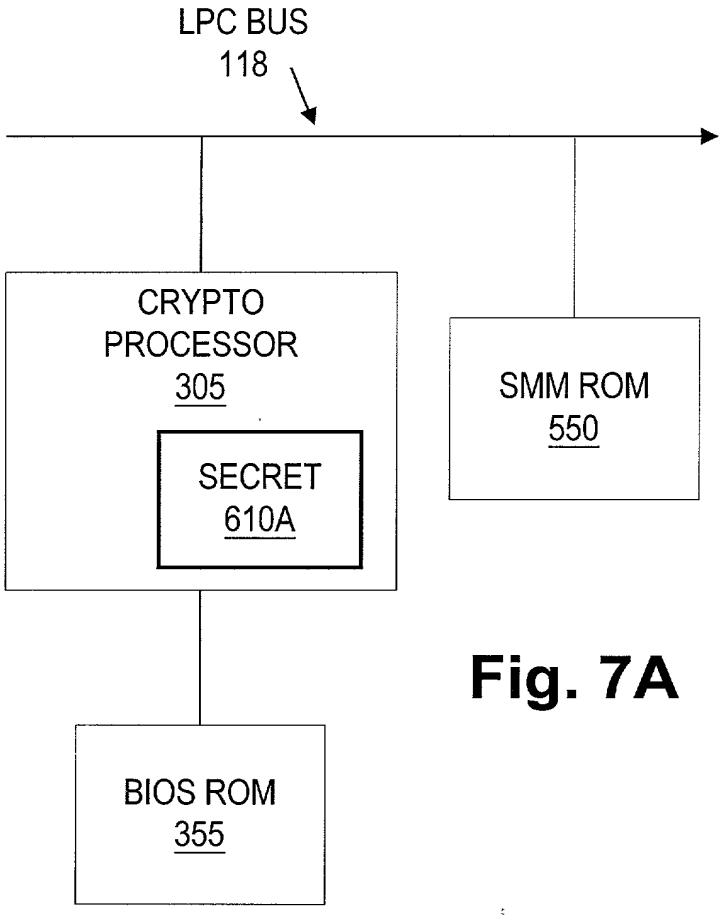

Fig. 7A

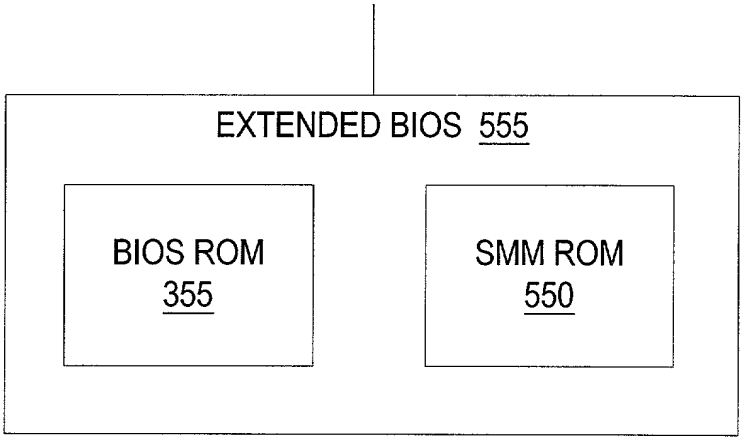

Fig. 7B

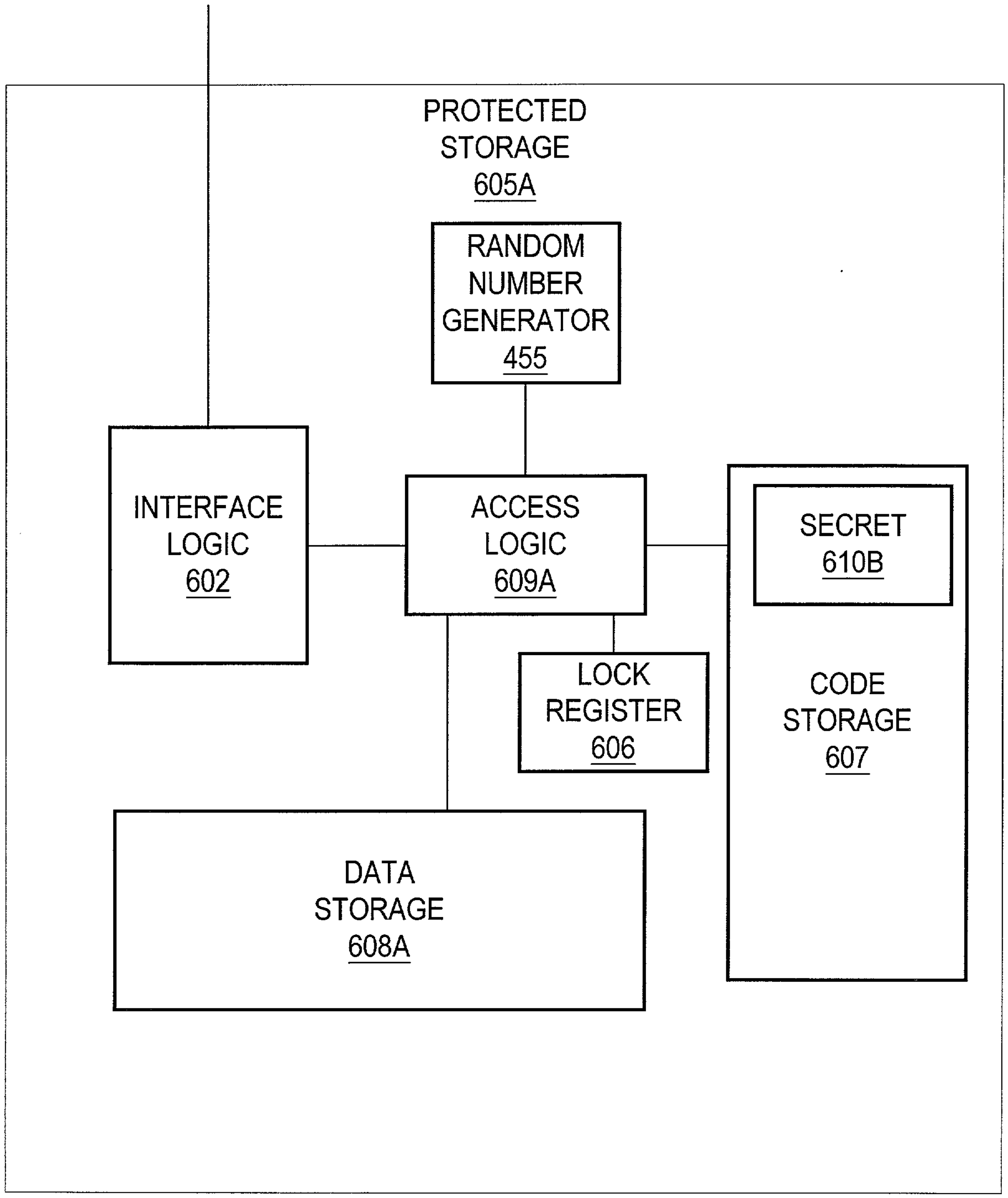

Fig. 7C

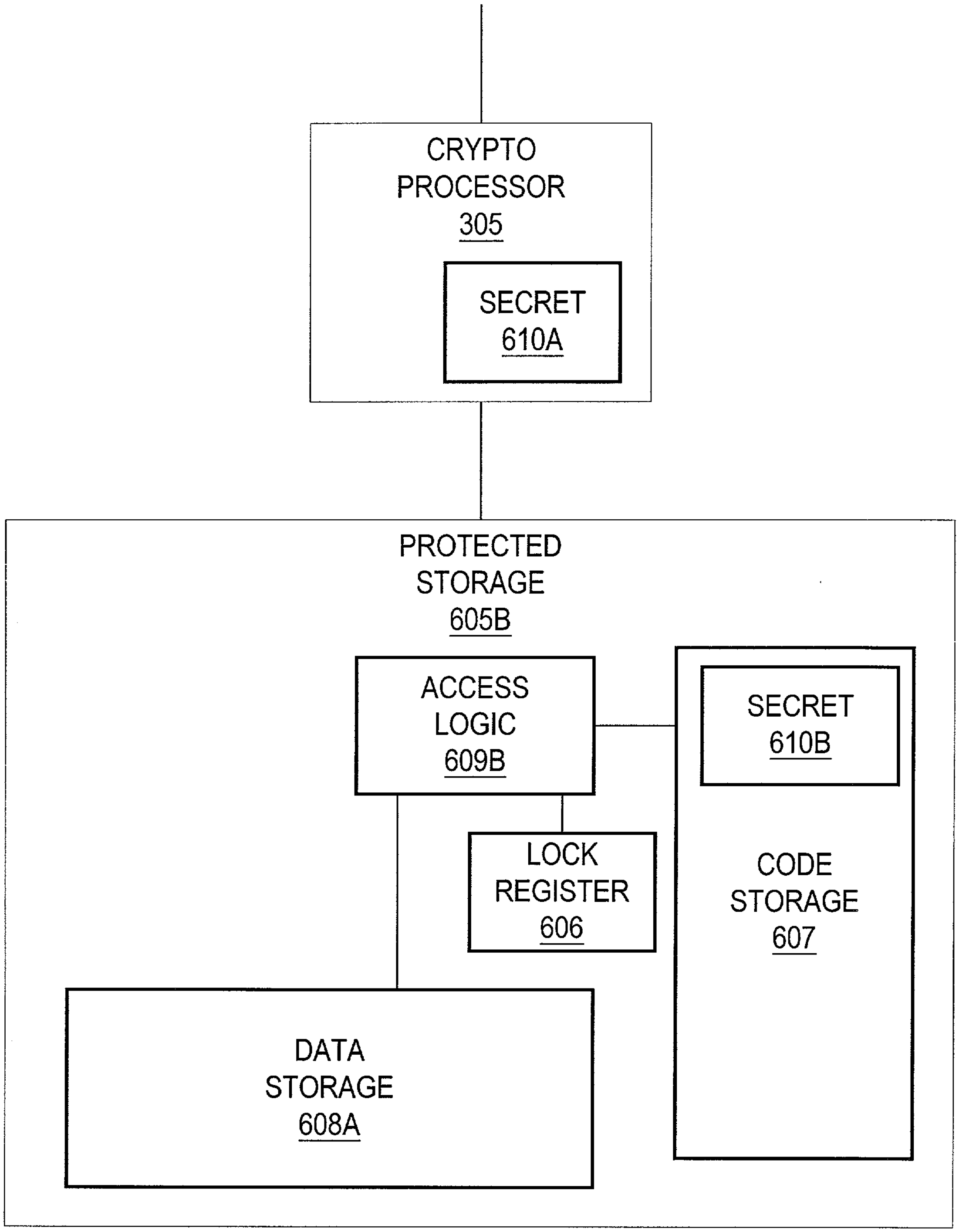

Fig. 7D

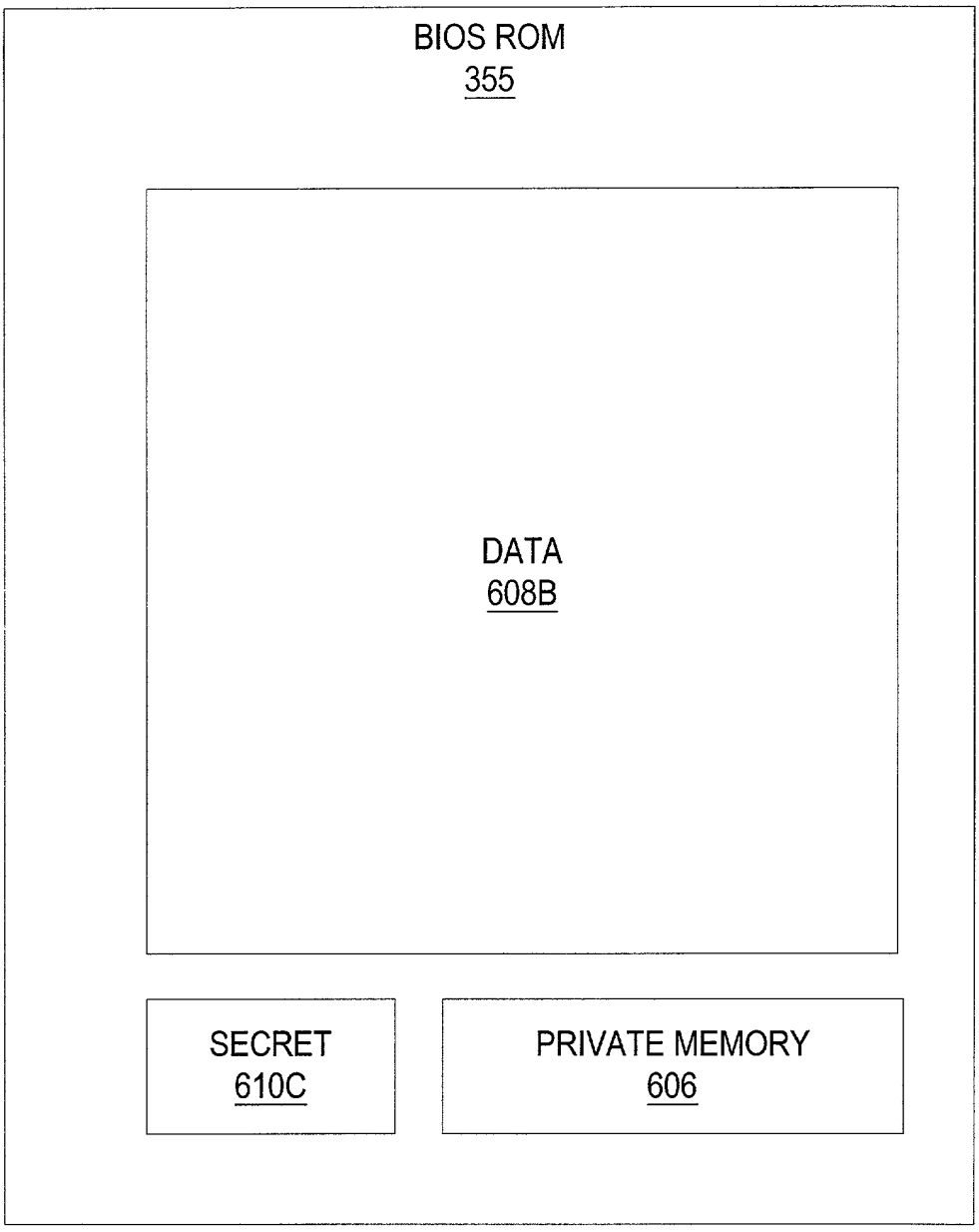

Fig. 8A

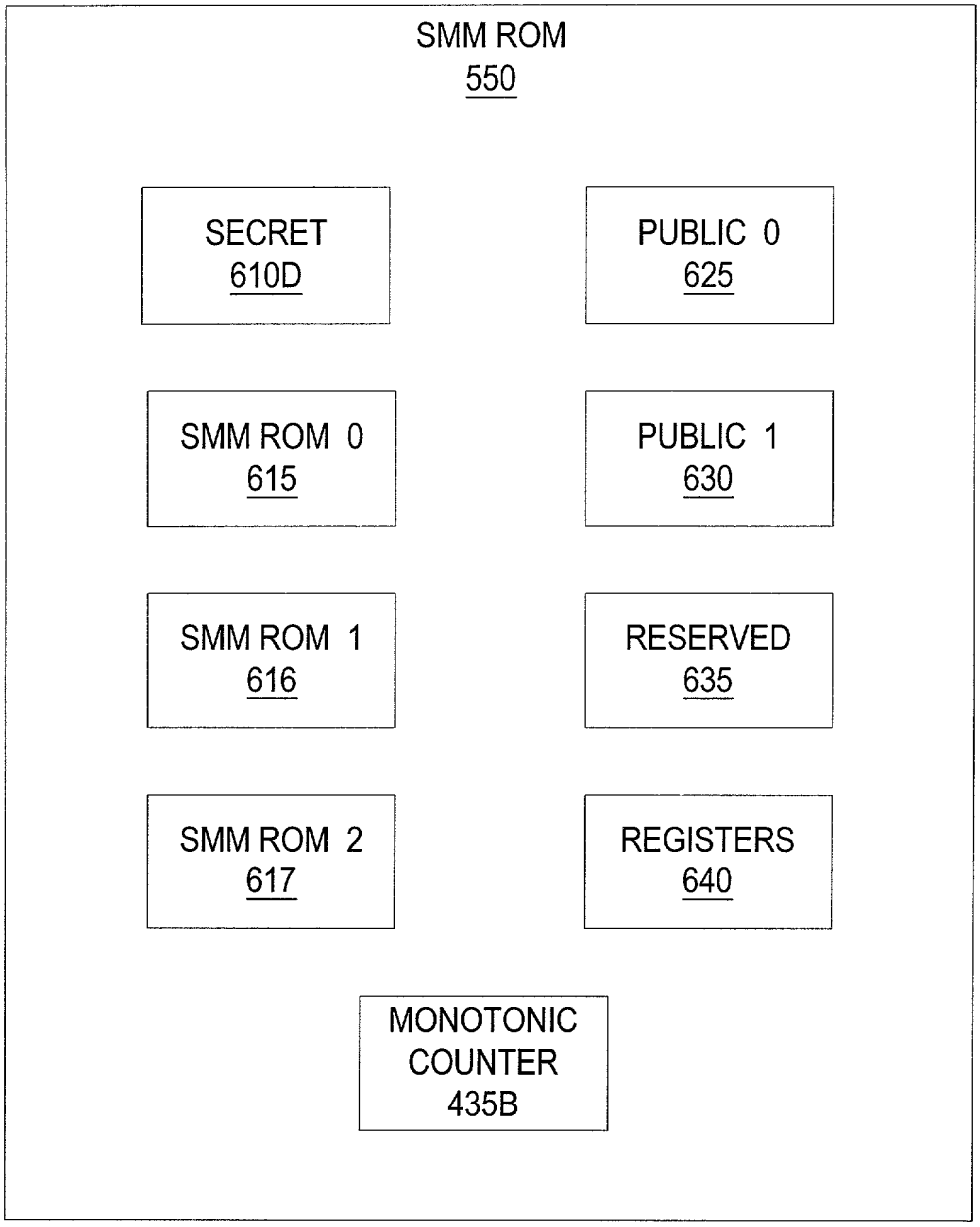

Fig. 8B

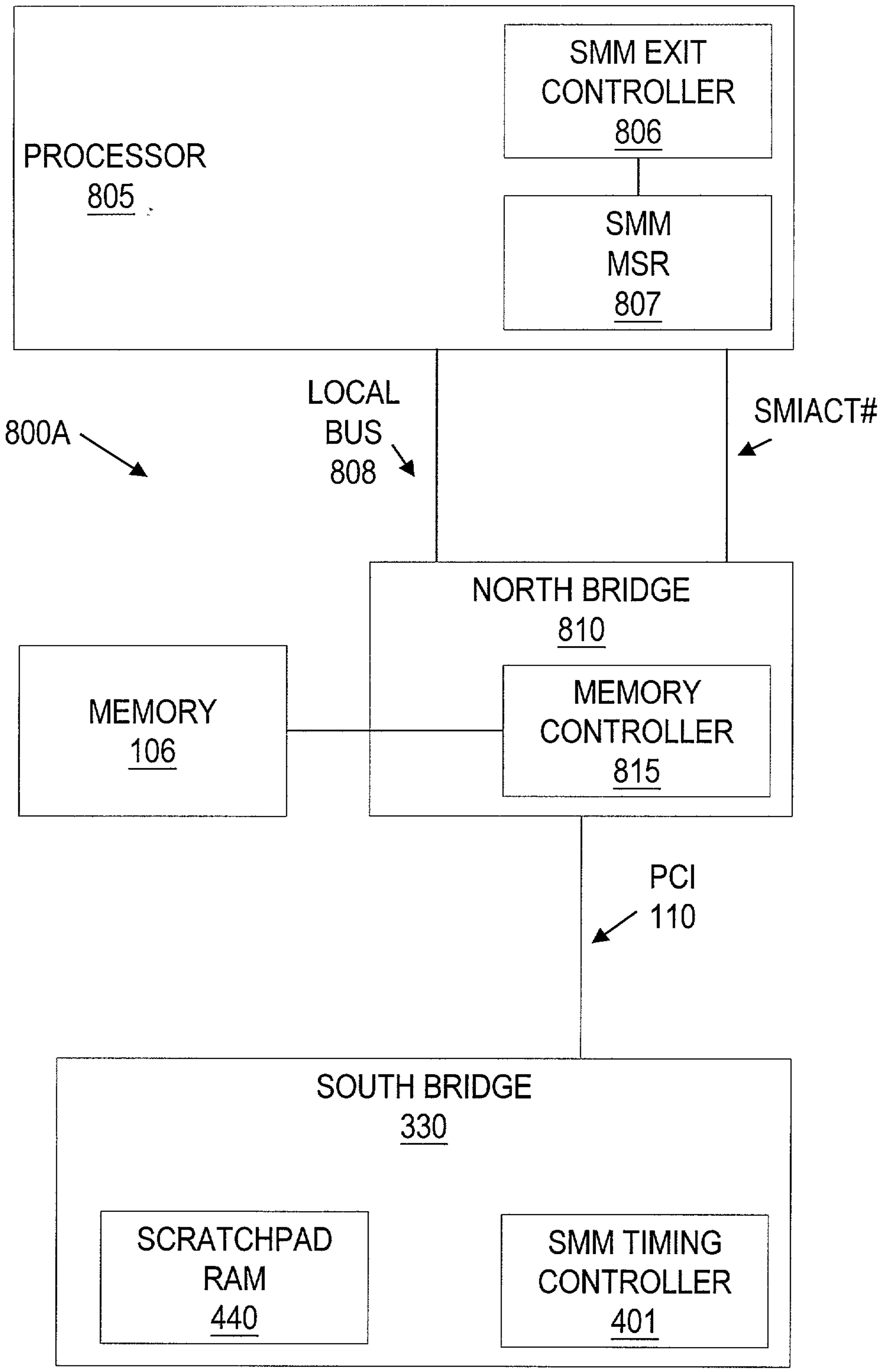

Fig. 9A

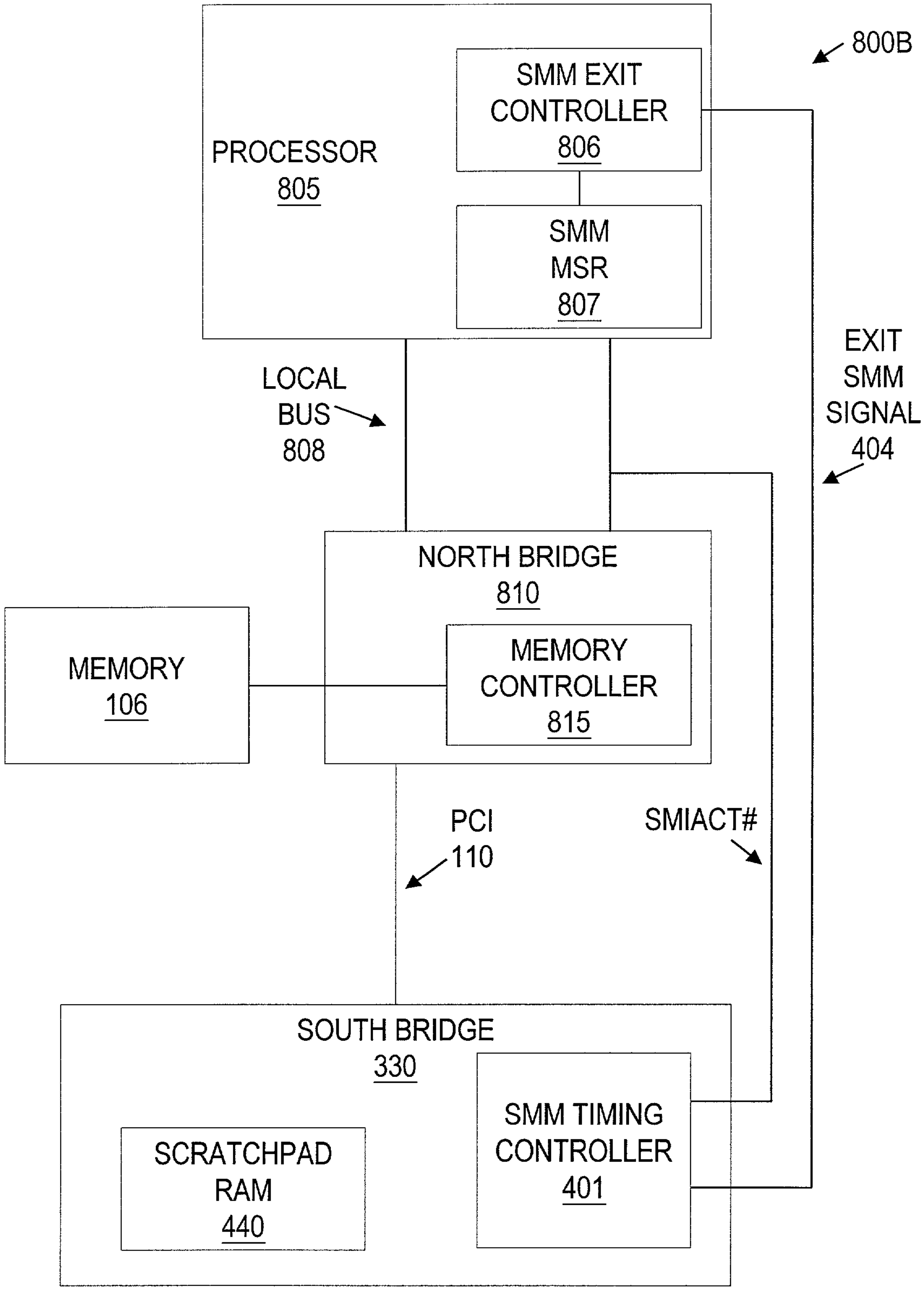

Fig. 9B

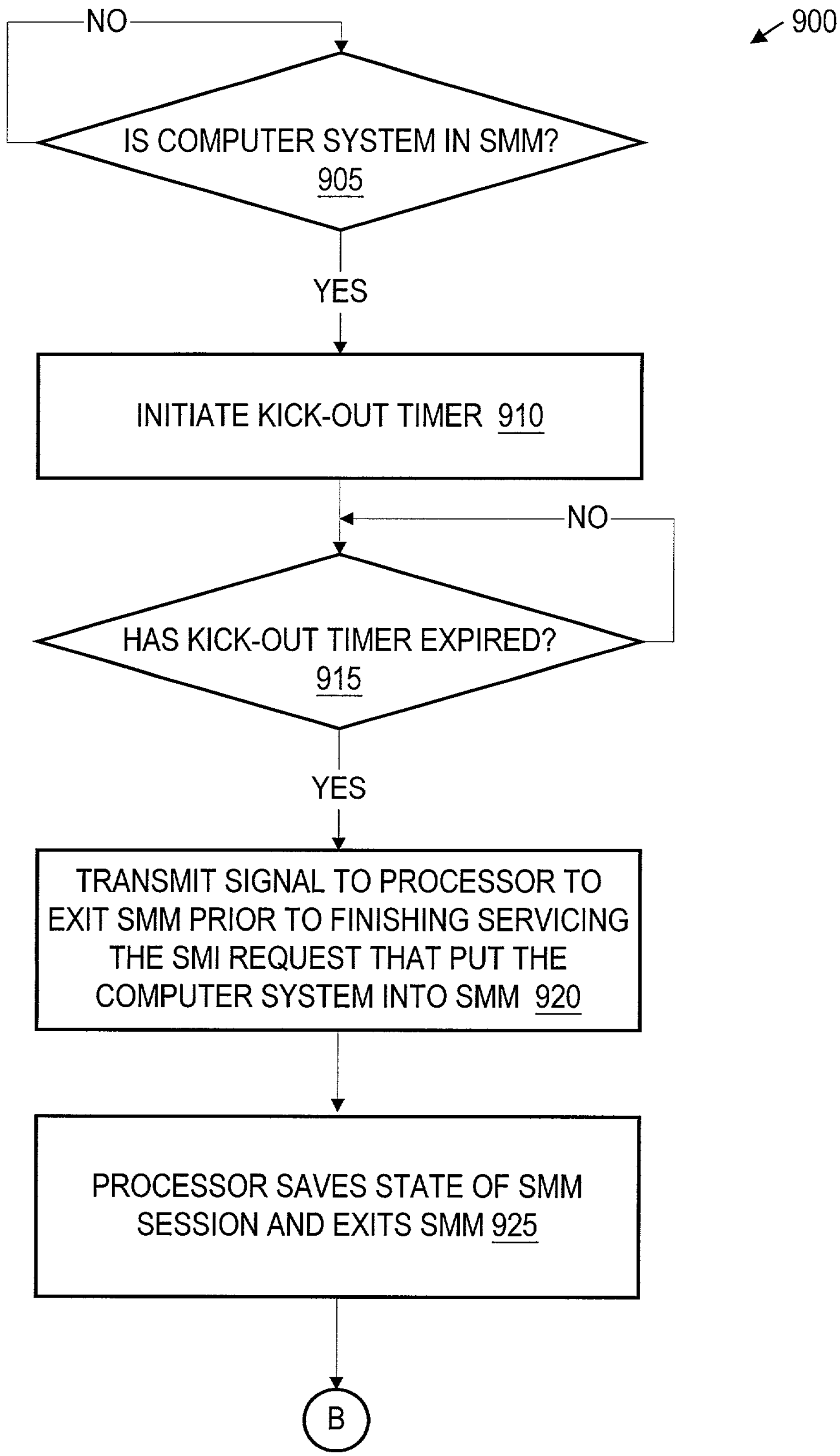

Fig. 10A

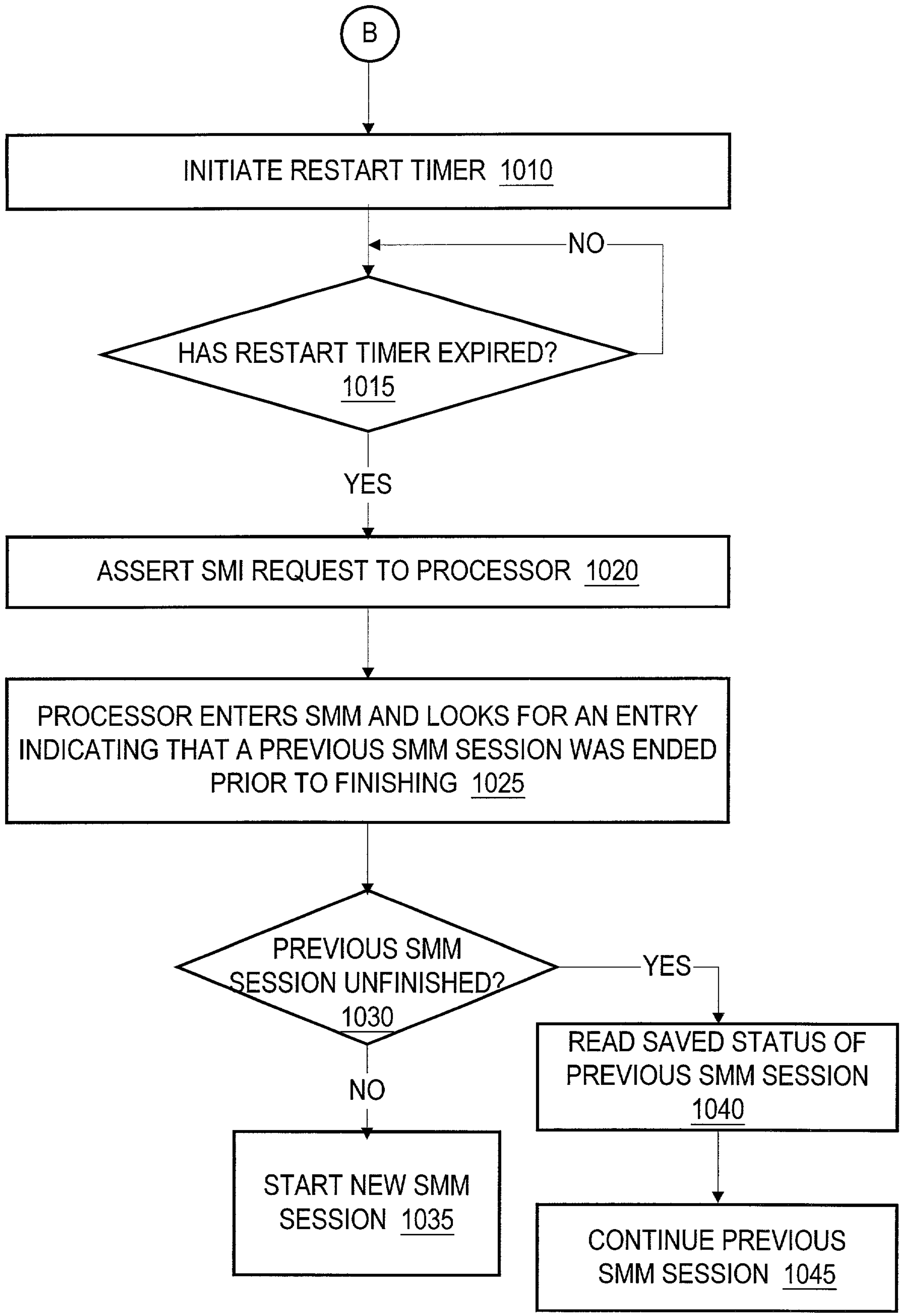

Fig. 10B

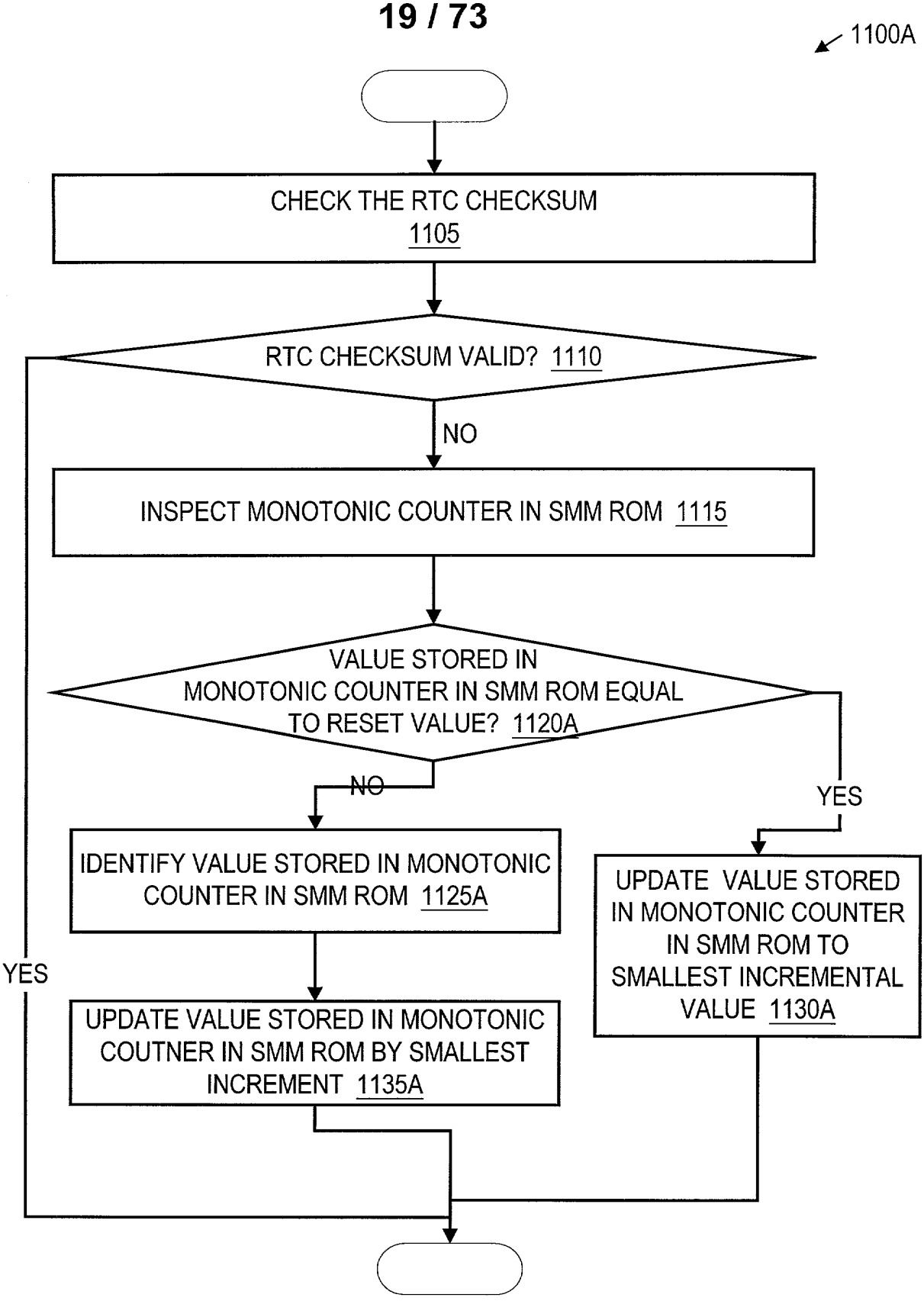

Fig. 11A

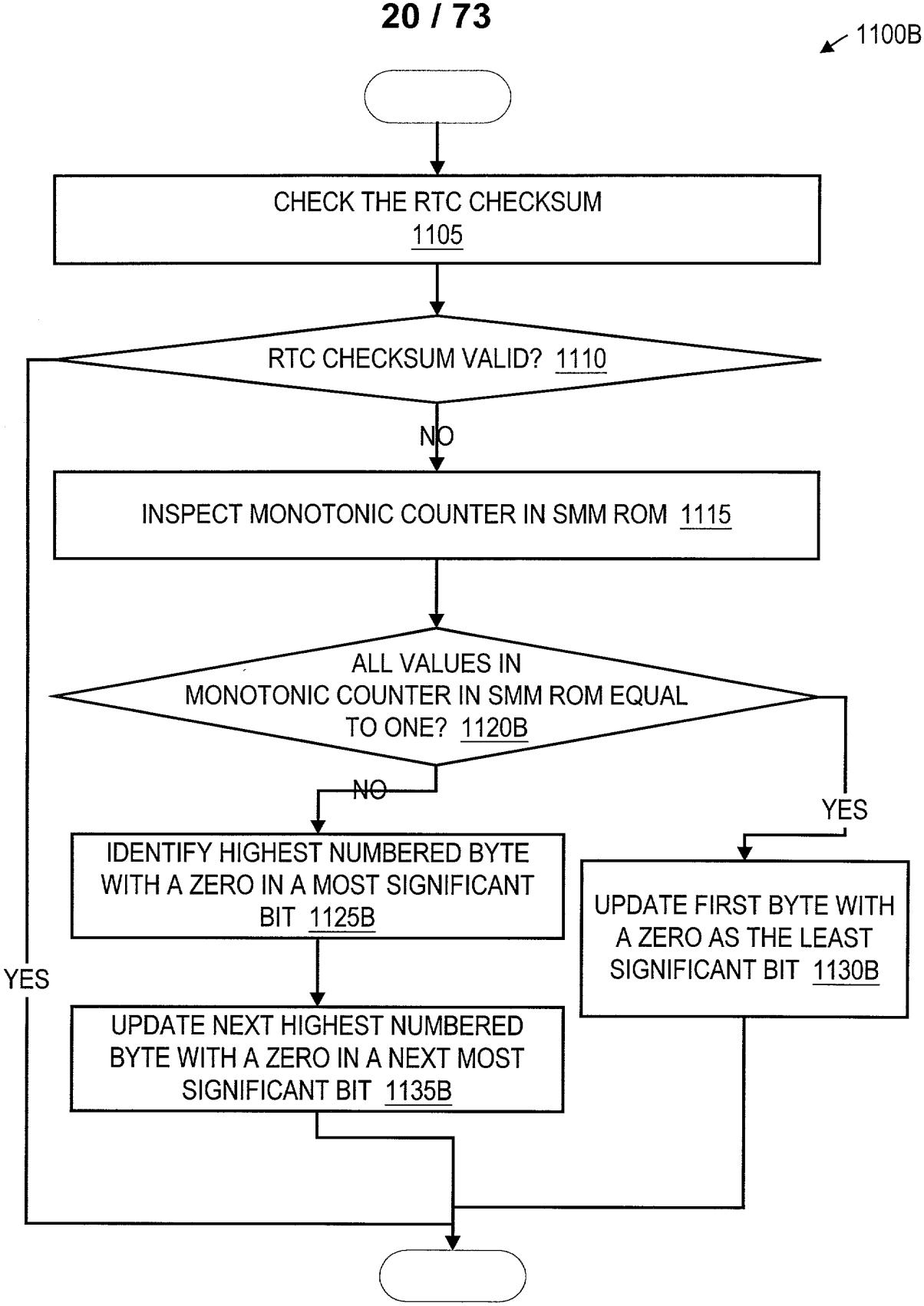

Fig. 11B

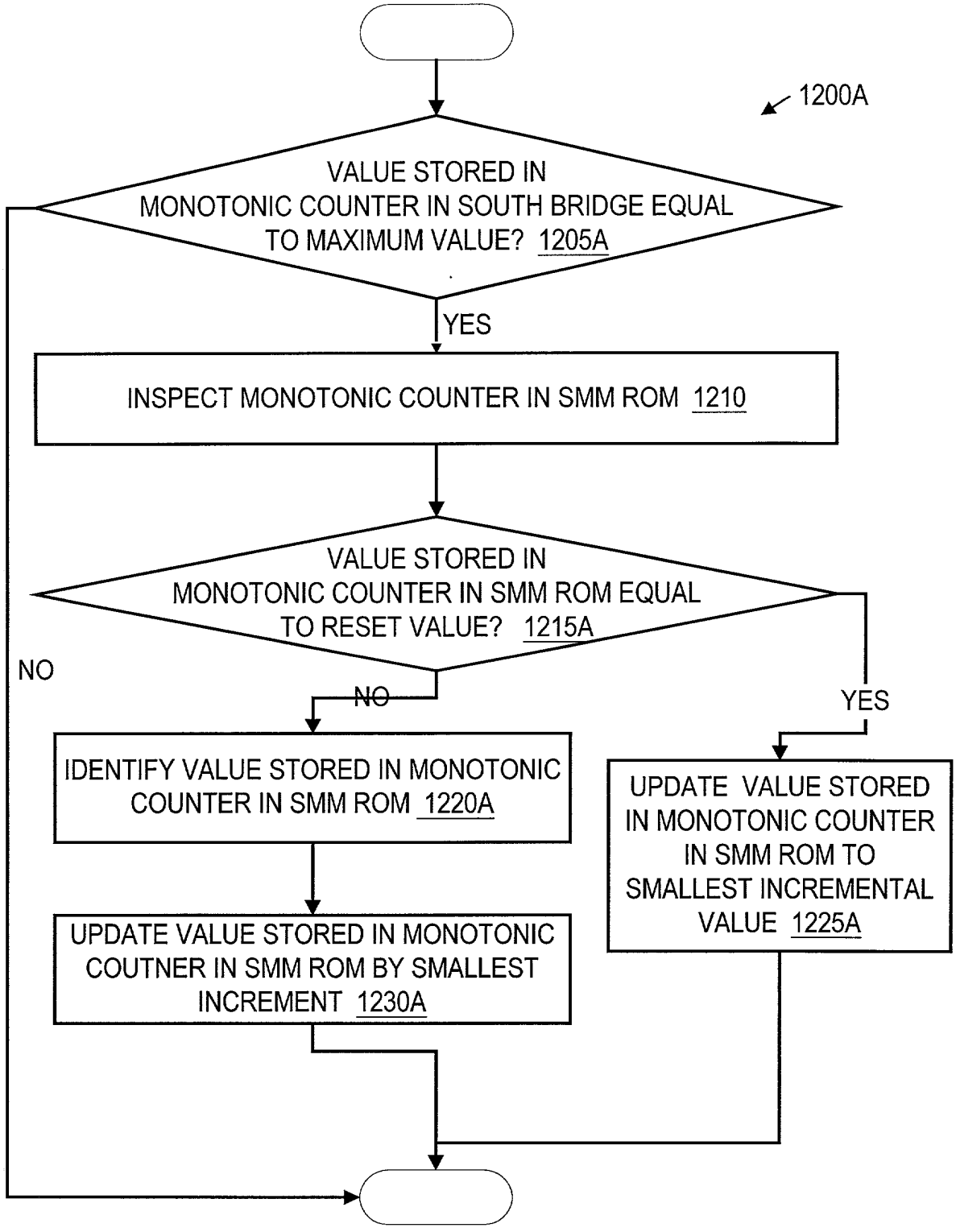
1200A
VALUE STORED IN MONOTONIC COUNTER IN SOUTH BRIDGE EQUAL TO MAXIMUM VALUE? 1205A
YES
INSPECT MONOTONIC COUNTER IN SMM ROM 1210
VALUE STORED IN MONOTONIC COUNTER IN SMM ROM EQUAL TO RESET VALUE? 1215A
NO
NO
YES
IDENTIFY VALUE STORED IN MONOTONIC COUNTER IN SMM ROM 1220A
UPDATE VALUE STORED IN MONOTONIC COUTNER IN SMM ROM BY SMALLEST INCREMENT 1230A
UPDATE VALUE STORED IN MONOTONIC COUNTER IN SMM ROM TO SMALLEST INCREMENTAL VALUE 1225A

Fig. 12A

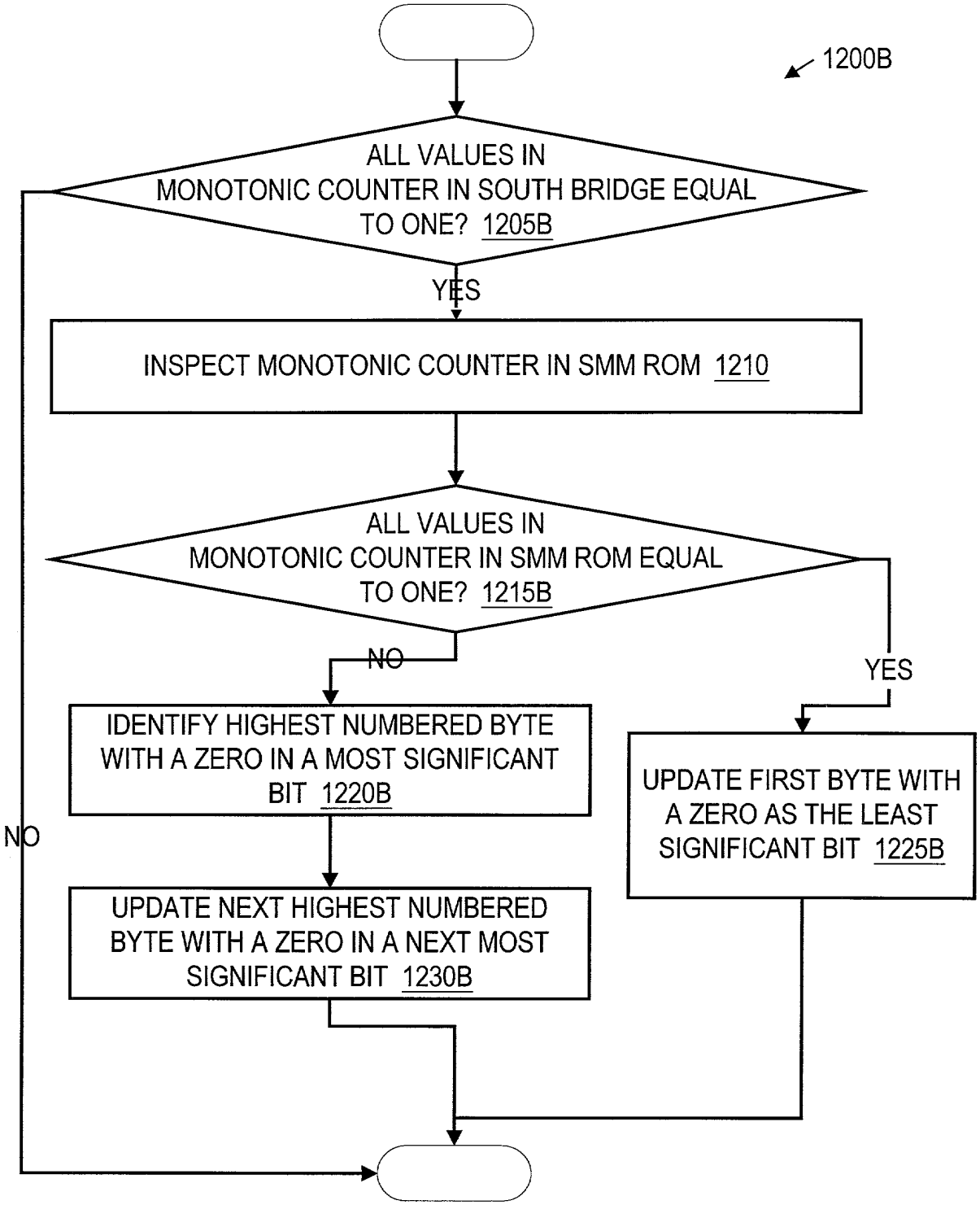
1200B
ALL VALUES IN MONOTONIC COUNTER IN SOUTH BRIDGE EQUAL TO ONE? 1205B
YES
INSPECT MONOTONIC COUNTER IN SMM ROM 1210
ALL VALUES IN MONOTONIC COUNTER IN SMM ROM EQUAL TO ONE? 1215B
NO
YES
IDENTIFY HIGHEST NUMBERED BYTE WITH A ZERO IN A MOST SIGNIFICANT BIT 1220B
UPDATE FIRST BYTE WITH A ZERO AS THE LEAST SIGNIFICANT BIT 1225B
NO
UPDATE NEXT HIGHEST NUMBERED BYTE WITH A ZERO IN A NEXT MOST SIGNIFICANT BIT 1230B

Fig. 12B

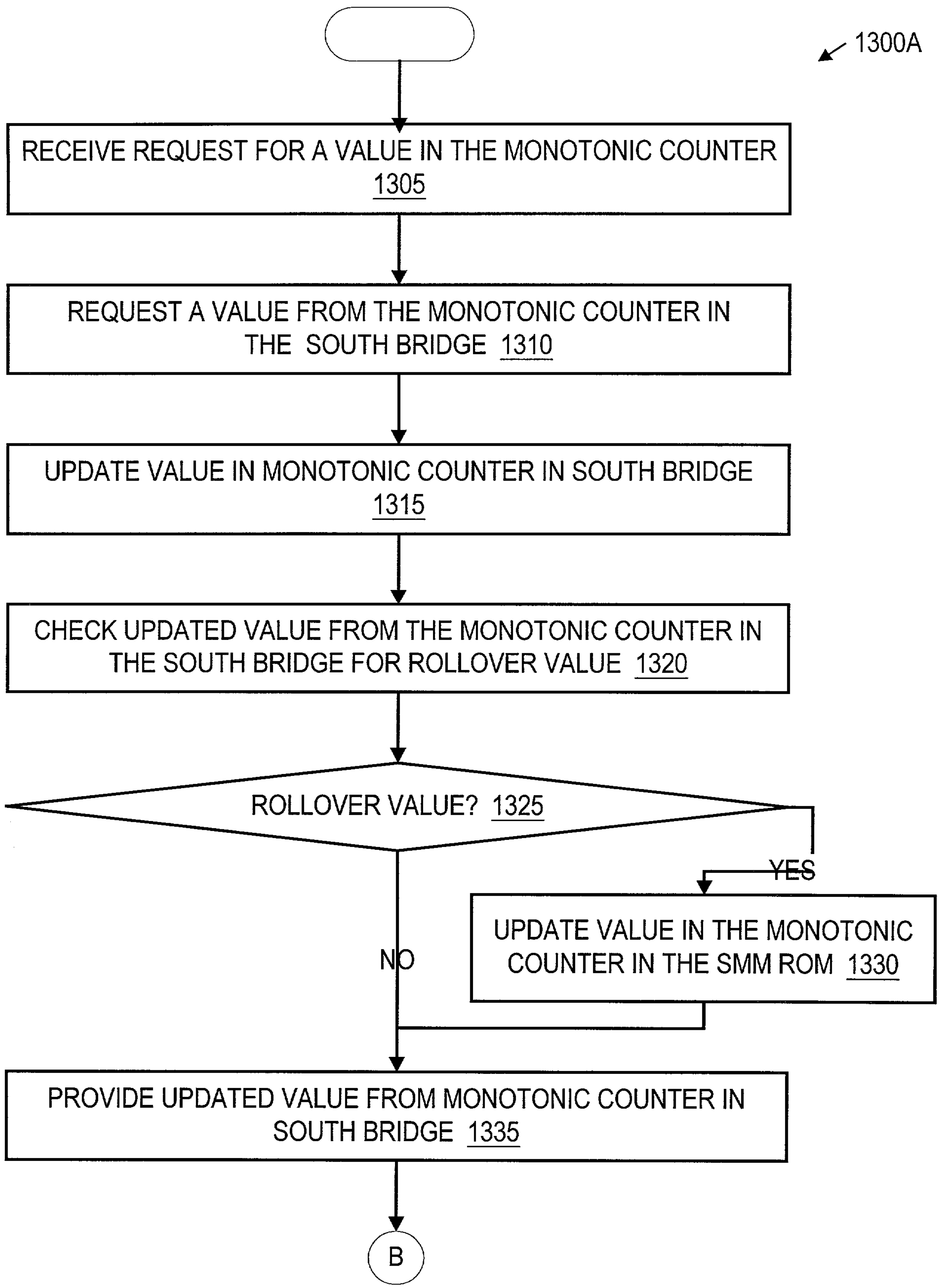

Fig. 13A

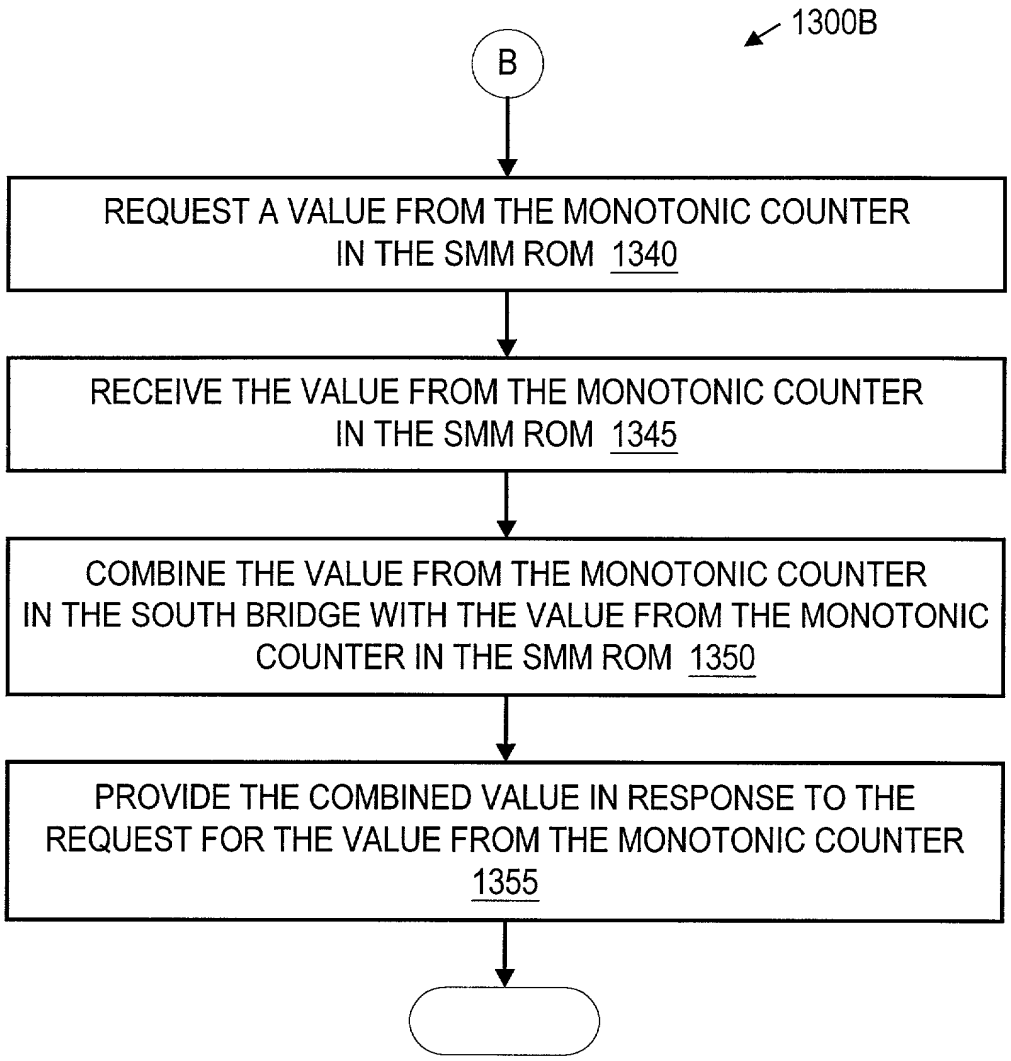
1300B
B
REQUEST A VALUE FROM THE MONOTONIC COUNTER IN THE SMM ROM 1340
RECEIVE THE VALUE FROM THE MONOTONIC COUNTER IN THE SMM ROM 1345
COMBINE THE VALUE FROM THE MONOTONIC COUNTER IN THE SOUTH BRIDGE WITH THE VALUE FROM THE MONOTONIC COUNTER IN THE SMM ROM 1350
PROVIDE THE COMBINED VALUE IN RESPONSE TO THE REQUEST FOR THE VALUE FROM THE MONOTONIC COUNTER 1355

Fig. 13B

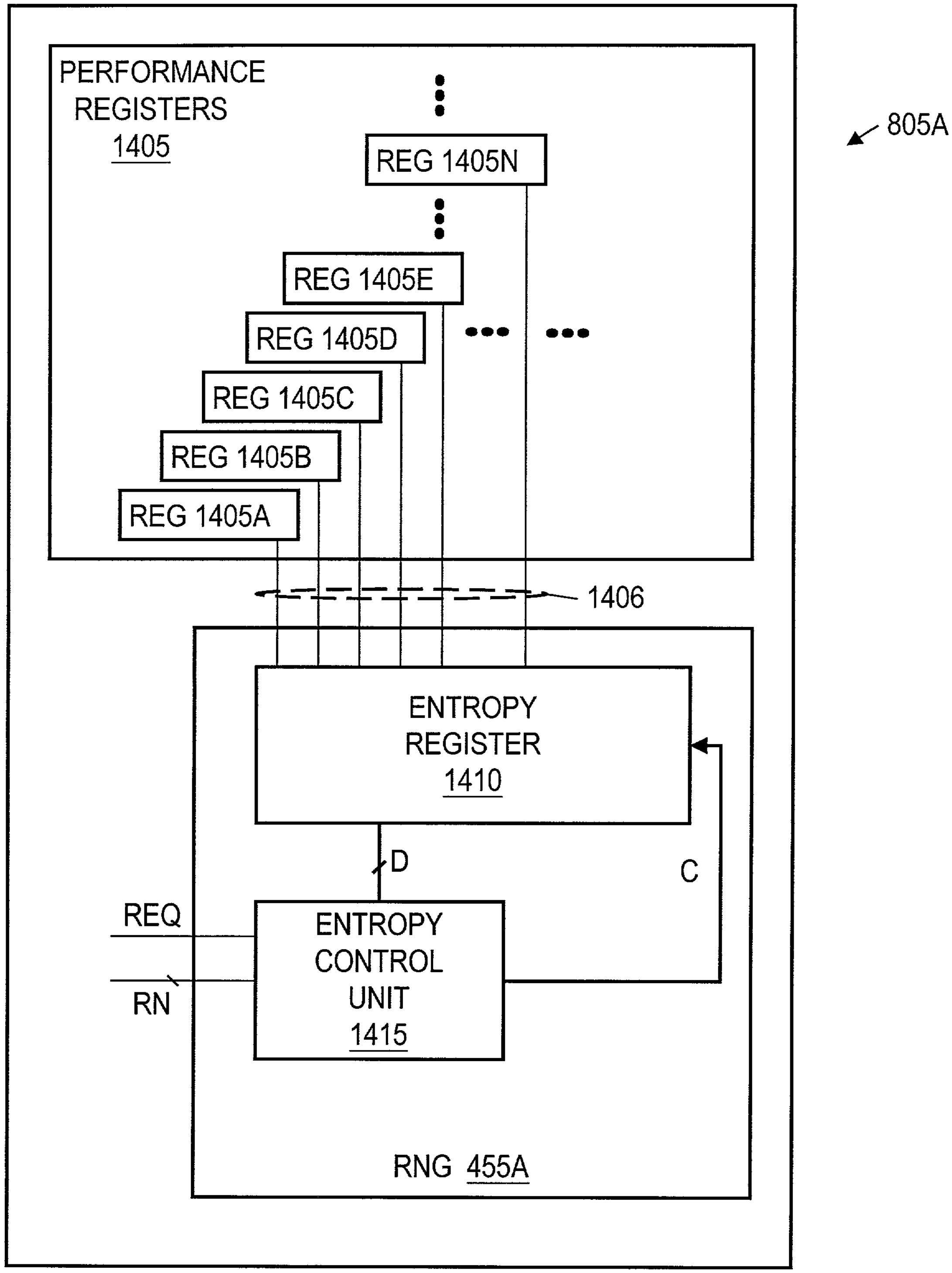

Fig. 14A

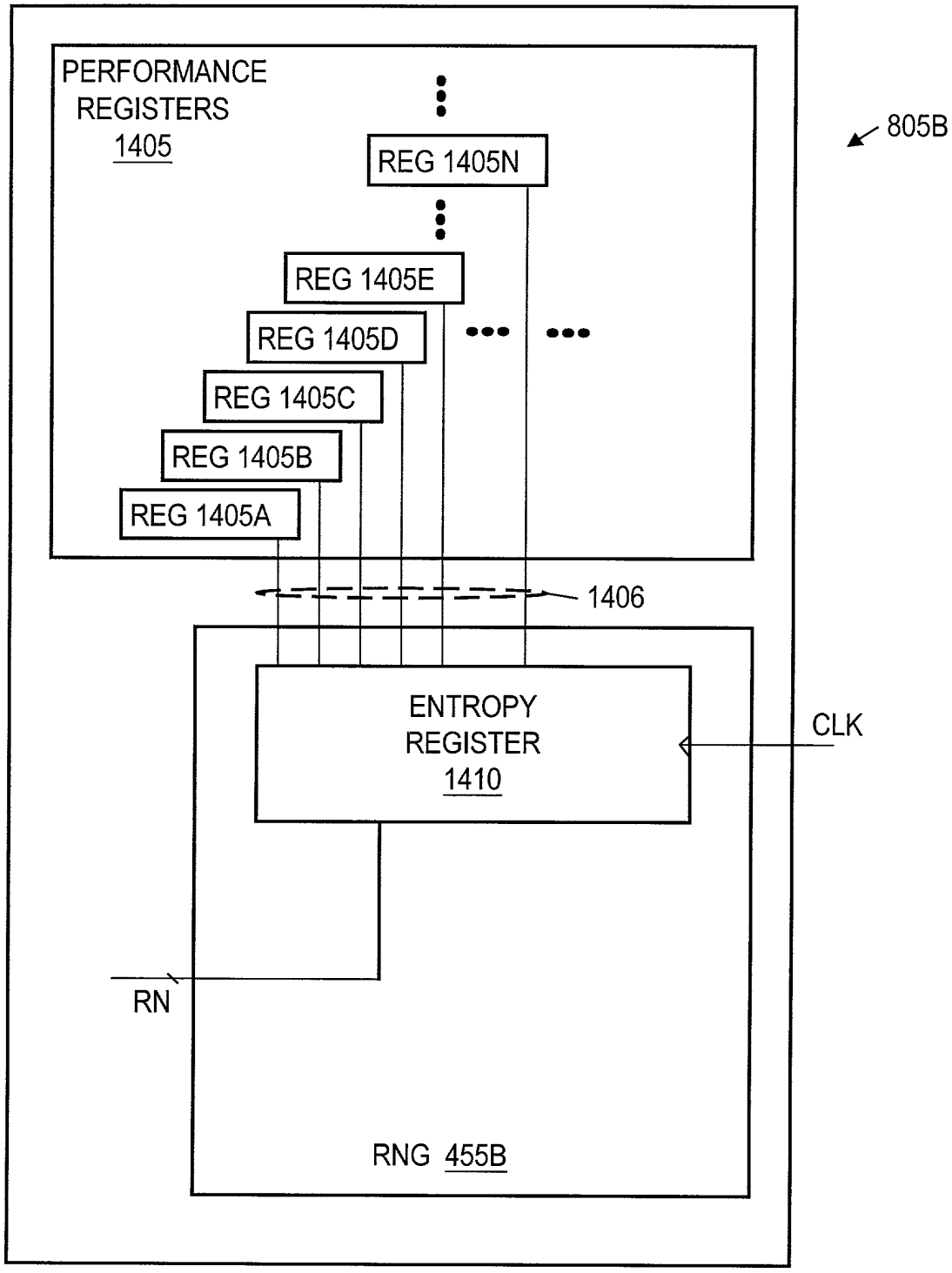

Fig. 14B

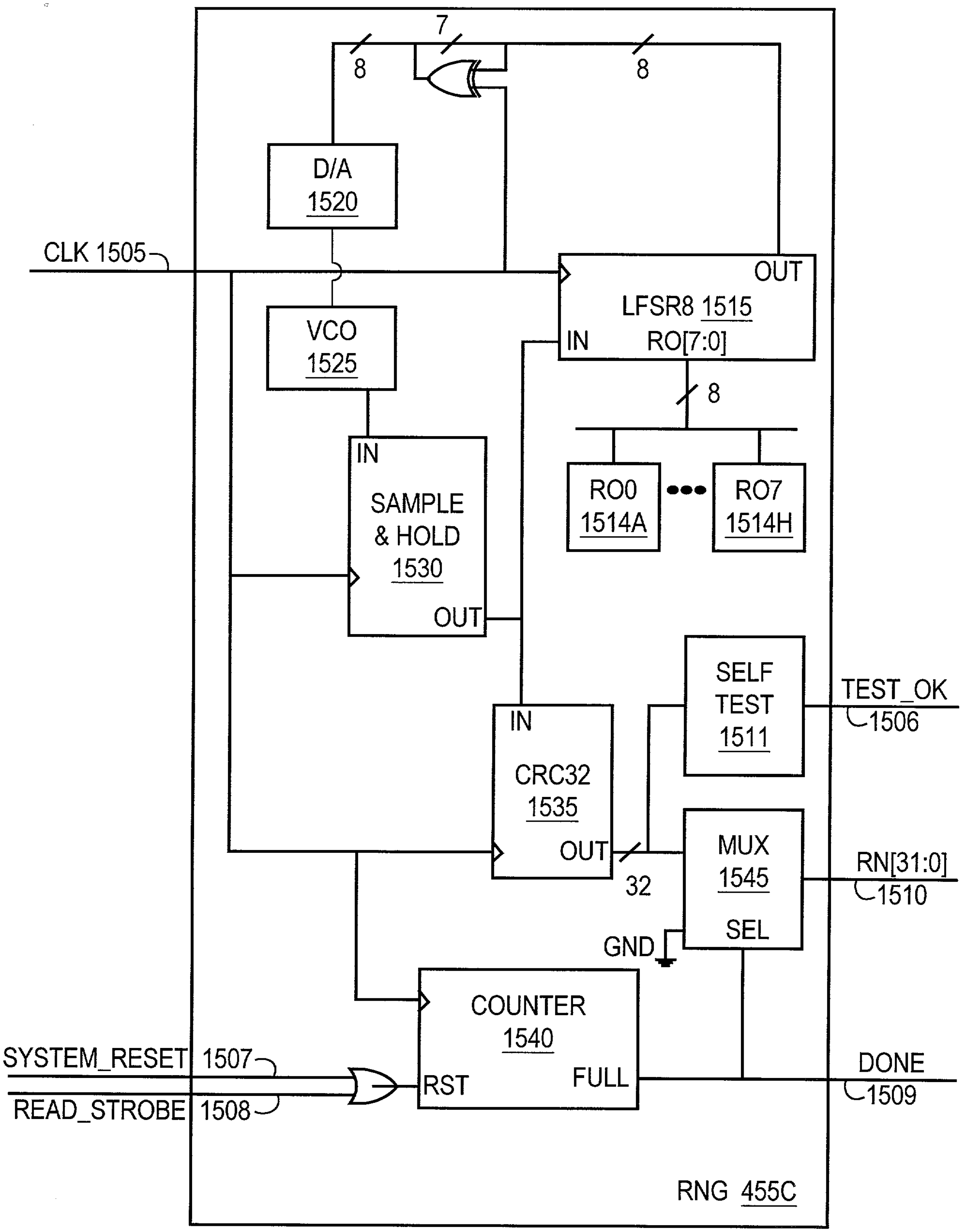

Fig. 15

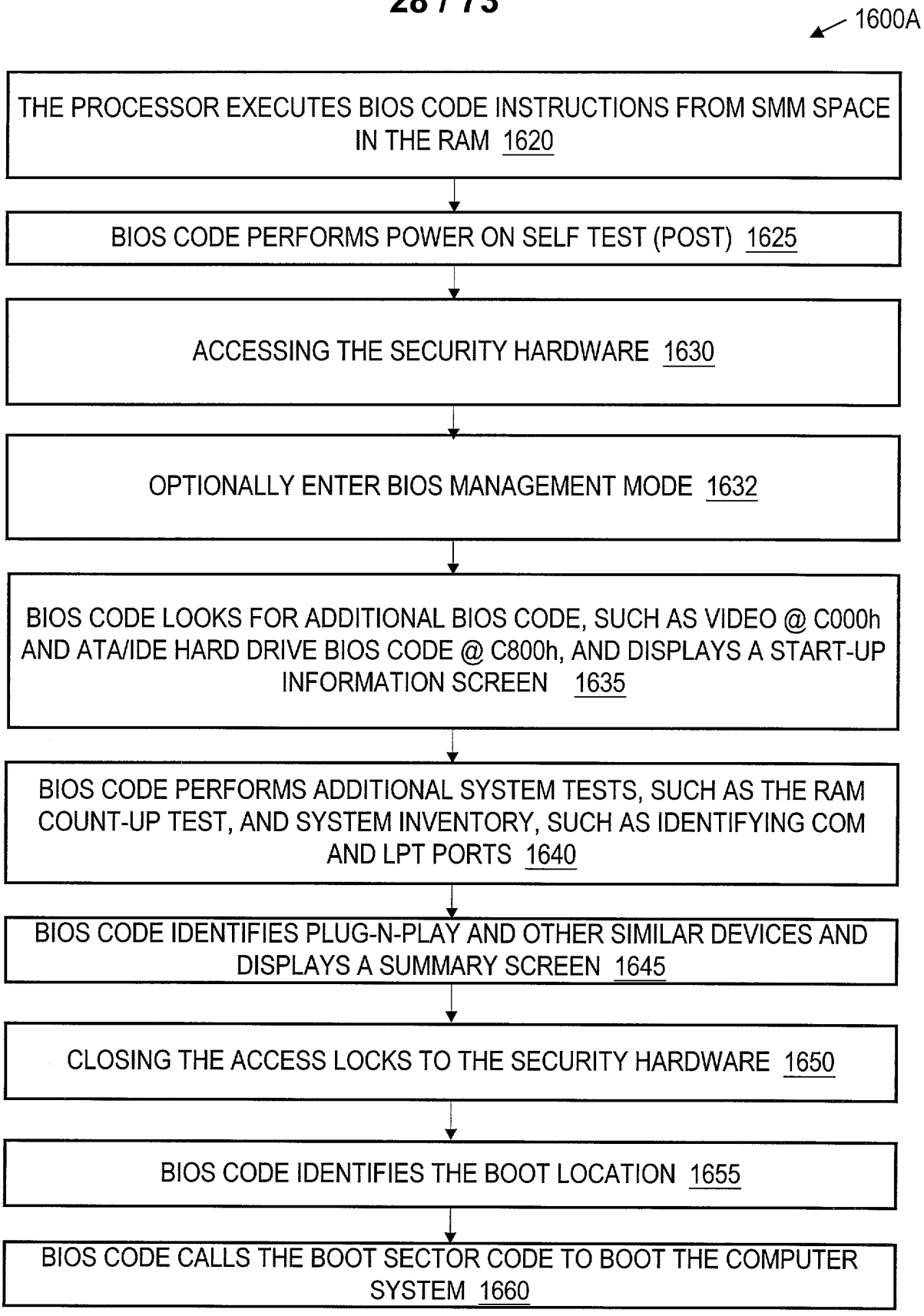

Fig. 16A

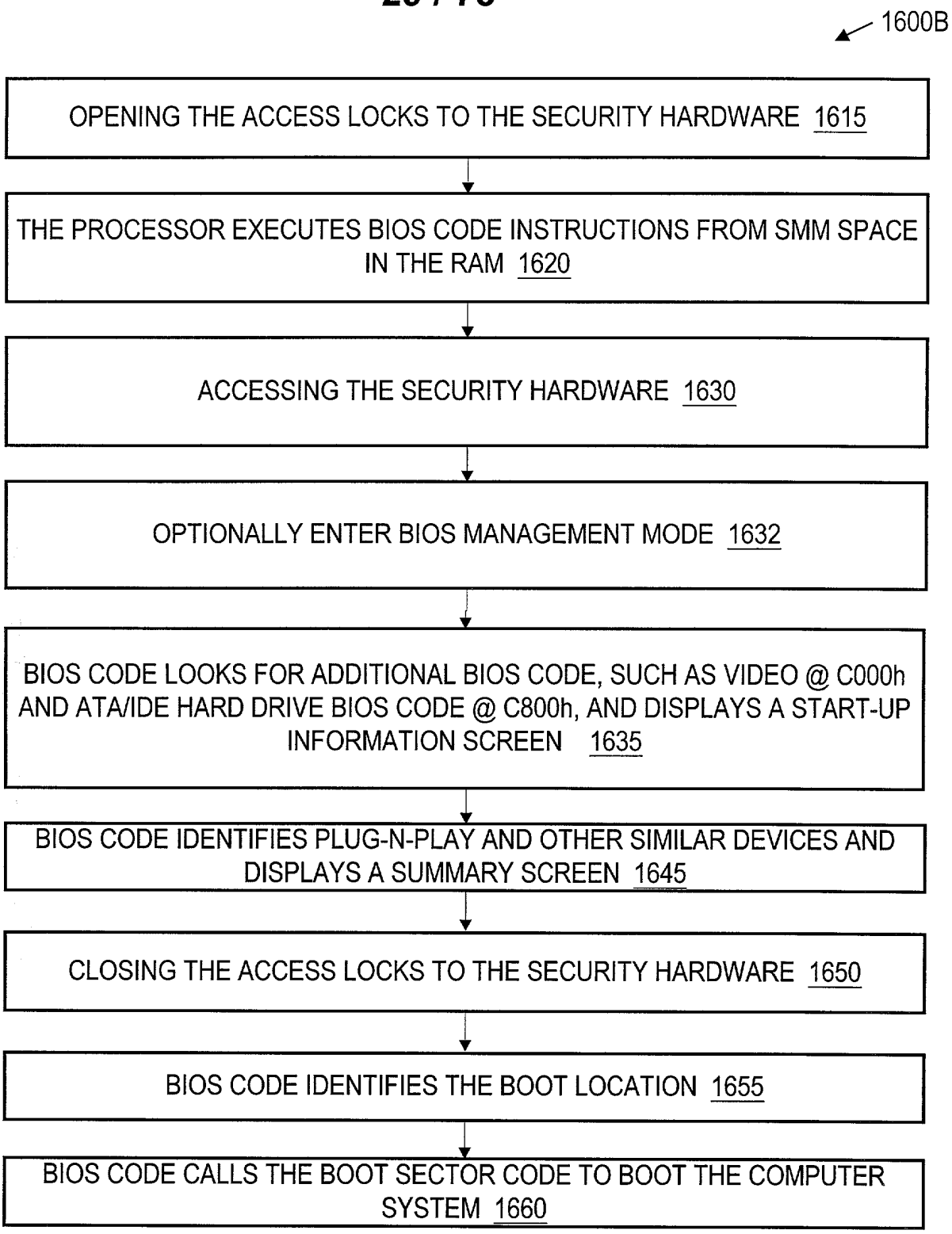
1600B
OPENING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1615
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM 1620
ACCESSING THE SECURITY HARDWARE 1630
OPTIONALLY ENTER BIOS MANAGEMENT MODE 1632
BIOS CODE LOOKS FOR ADDITIONAL BIOS CODE, SUCH AS VIDEO @ C000h AND ATA/IDE HARD DRIVE BIOS CODE @ C800h, AND DISPLAYS A START-UP INFORMATION SCREEN 1635
BIOS CODE IDENTIFIES PLUG-N-PLAY AND OTHER SIMILAR DEVICES AND DISPLAYS A SUMMARY SCREEN 1645
CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650
BIOS CODE IDENTIFIES THE BOOT LOCATION 1655
BIOS CODE CALLS THE BOOT SECTOR CODE TO BOOT THE COMPUTER SYSTEM 1660

Fig. 16B

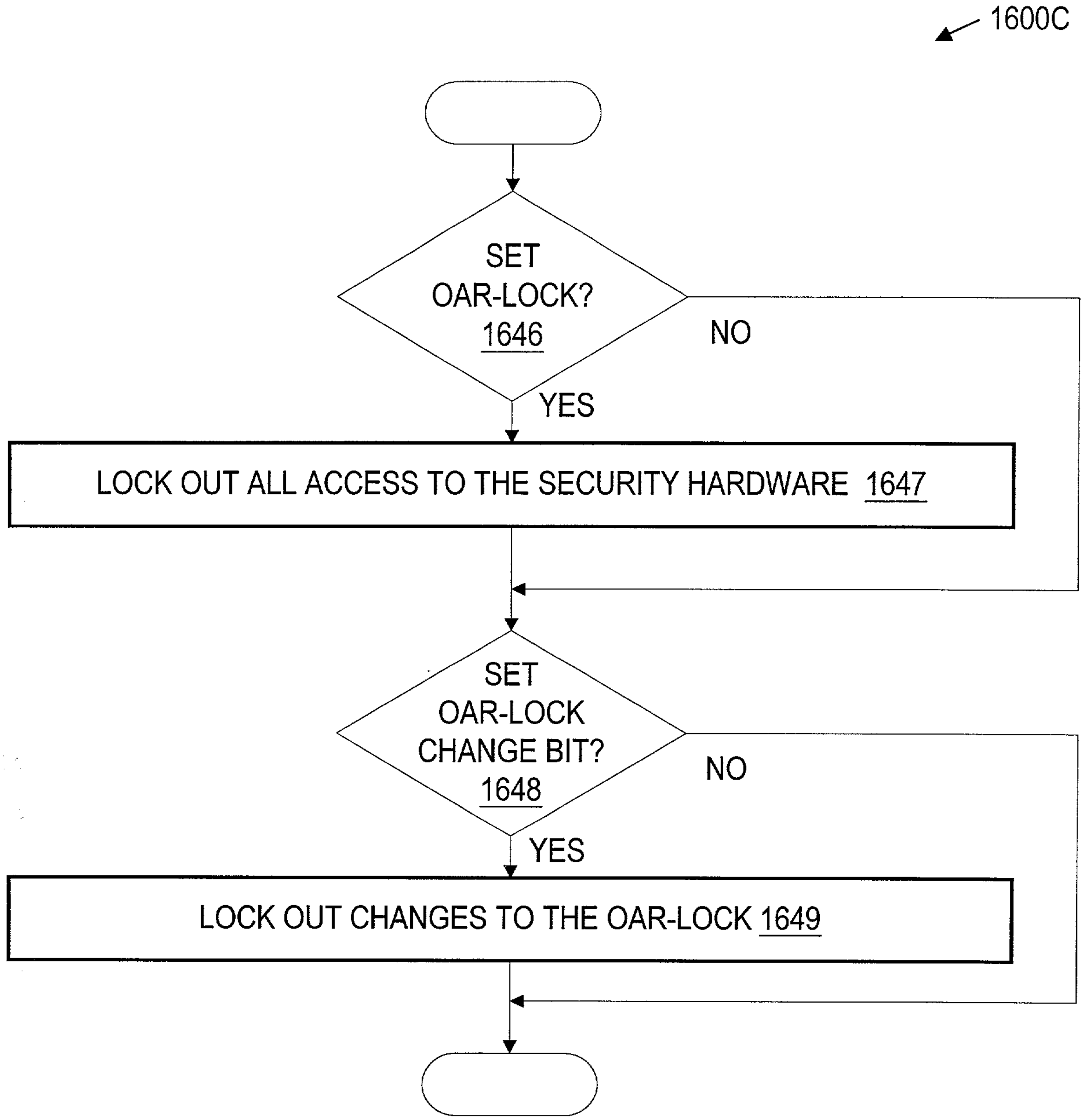
1600C
SET OAR-LOCK? 1646
NO
YES
LOCK OUT ALL ACCESS TO THE SECURITY HARDWARE 1647
SET OAR-LOCK CHANGE BIT? 1648
NO
YES
LOCK OUT CHANGES TO THE OAR-LOCK 1649

Fig. 16C

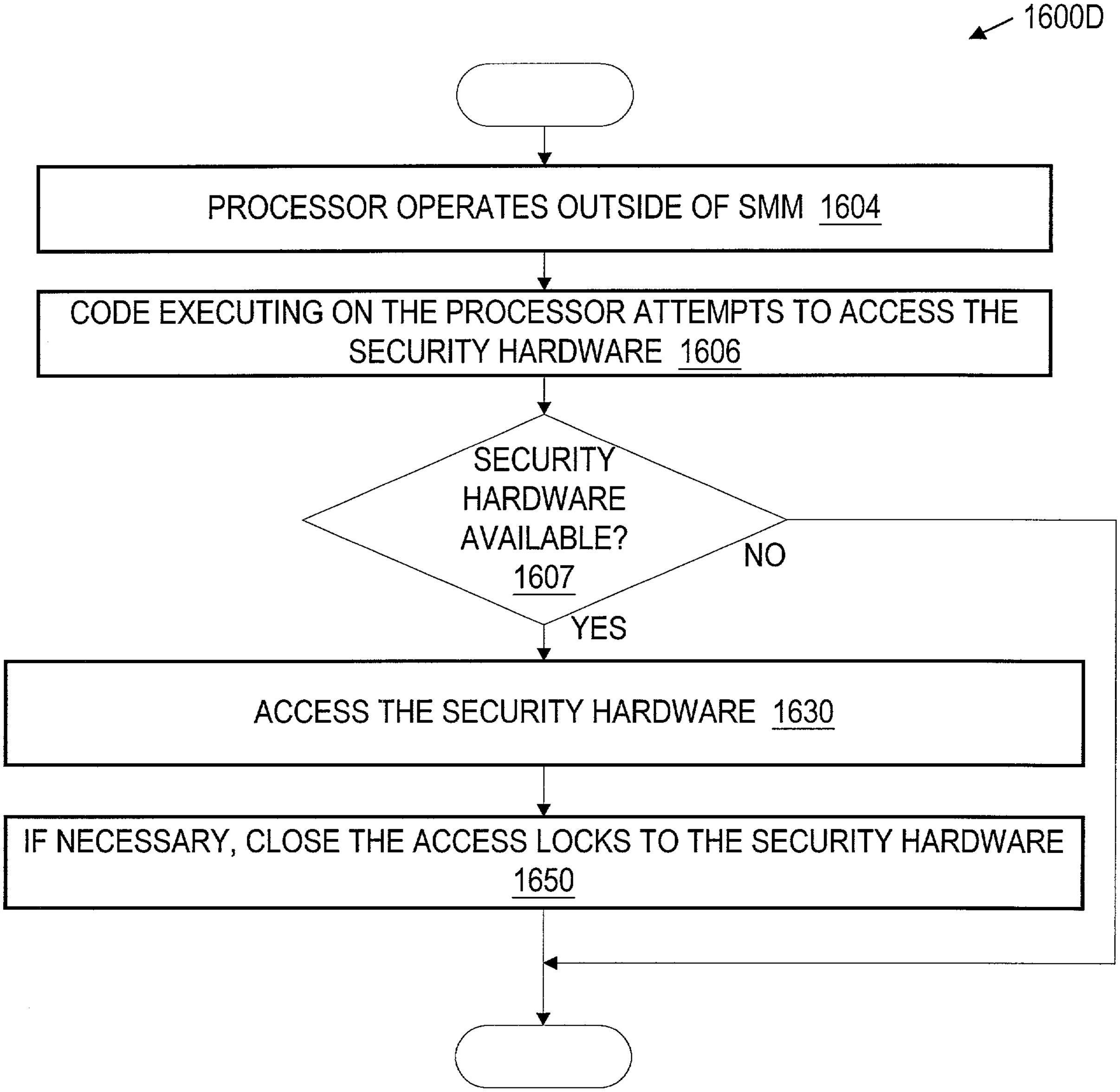

Fig. 16D

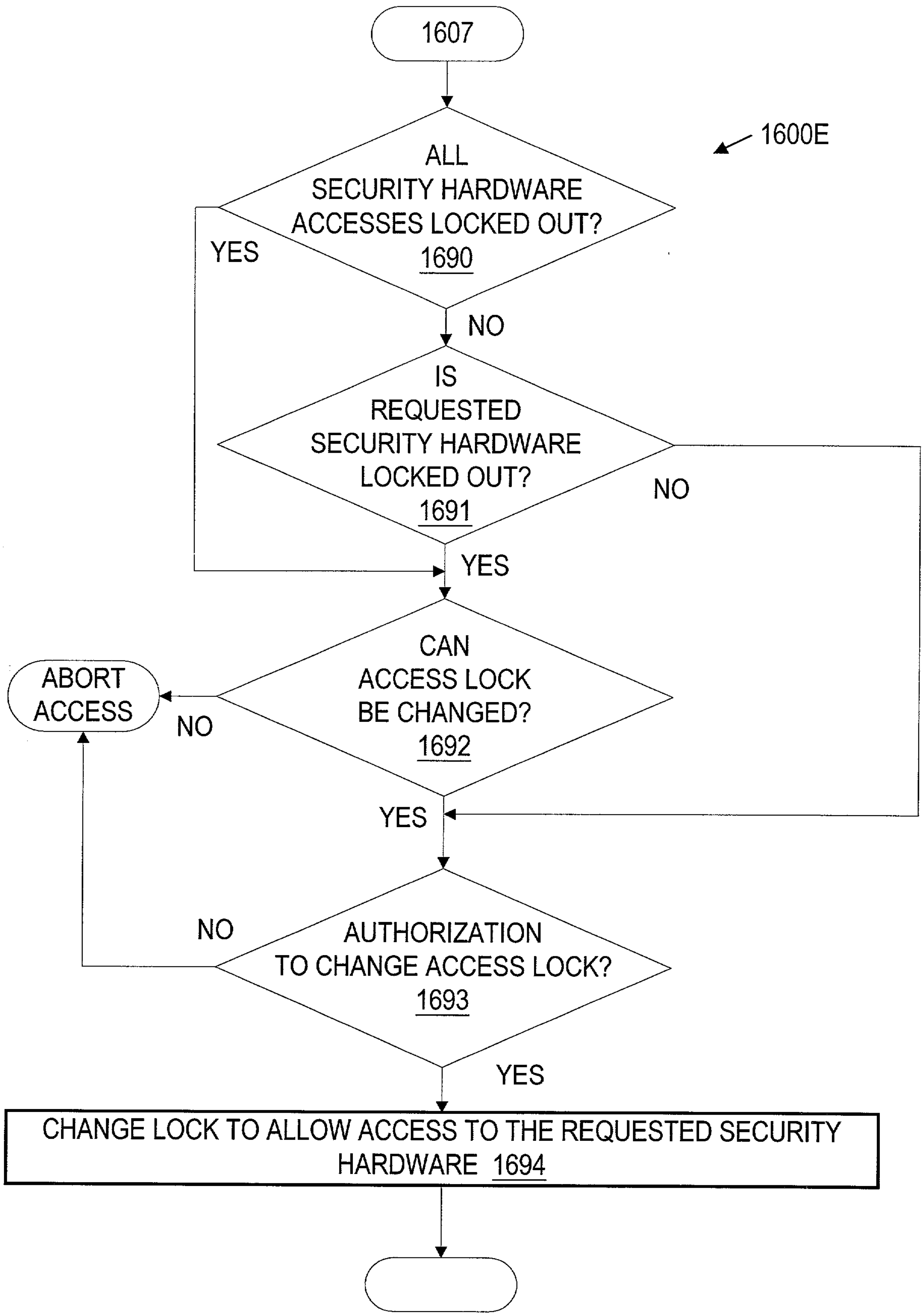

Fig. 16E

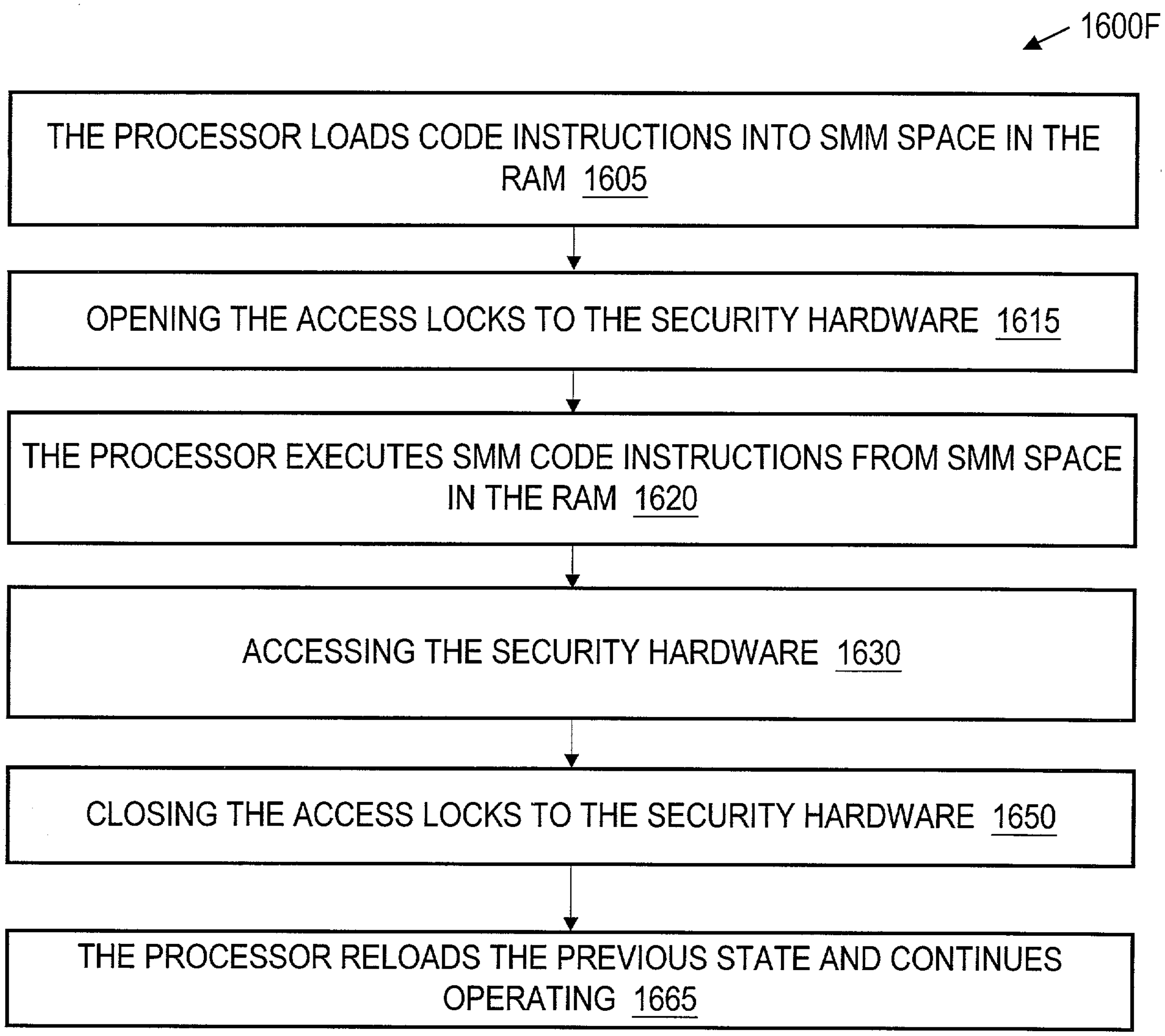

Fig. 16F

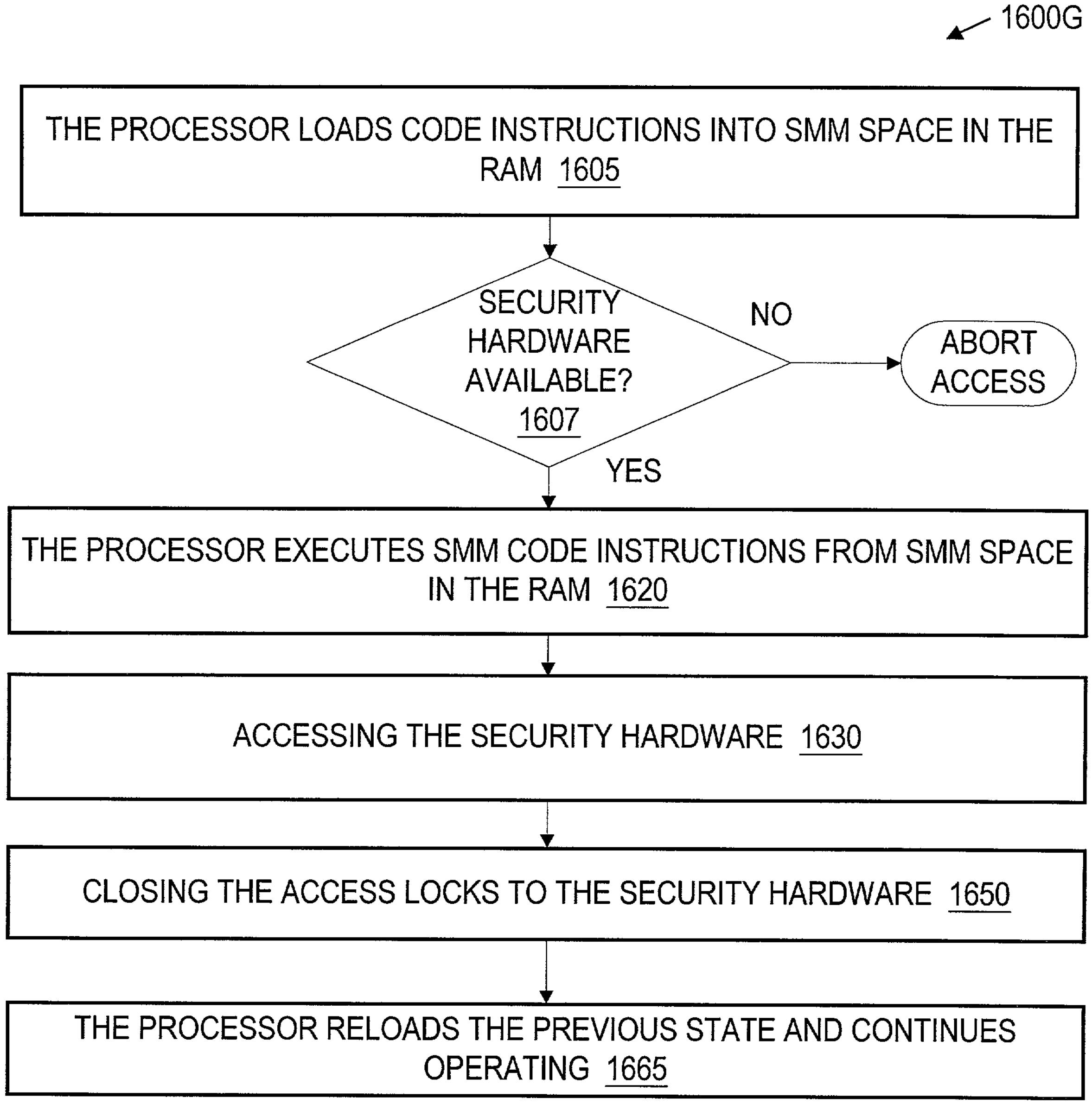
1600G
THE PROCESSOR LOADS CODE INSTRUCTIONS INTO SMM SPACE IN THE RAM 1605
SECURITY HARDWARE AVAILABLE? 1607
NO
ABORT ACCESS
YES
THE PROCESSOR EXECUTES SMM CODE INSTRUCTIONS FROM SMM SPACE IN THE RAM 1620
ACCESSING THE SECURITY HARDWARE 1630
CLOSING THE ACCESS LOCKS TO THE SECURITY HARDWARE 1650
THE PROCESSOR RELOADS THE PREVIOUS STATE AND CONTINUES OPERATING 1665

Fig. 16G

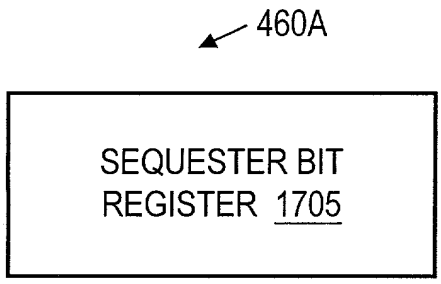

Fig. 17A

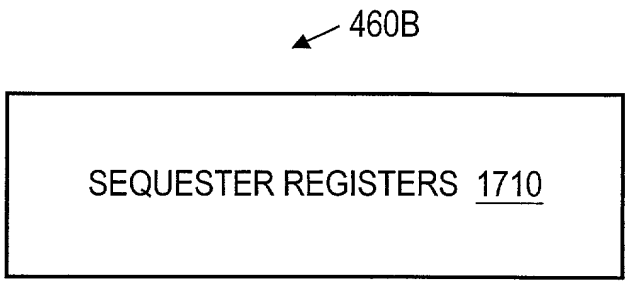

Fig. 17B

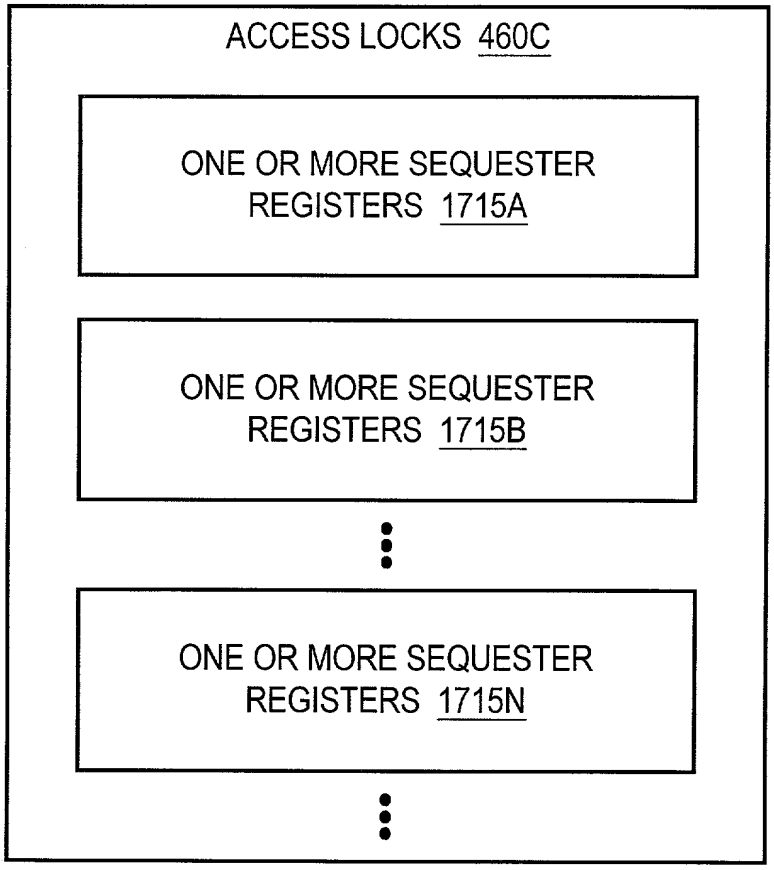

Fig. 17C

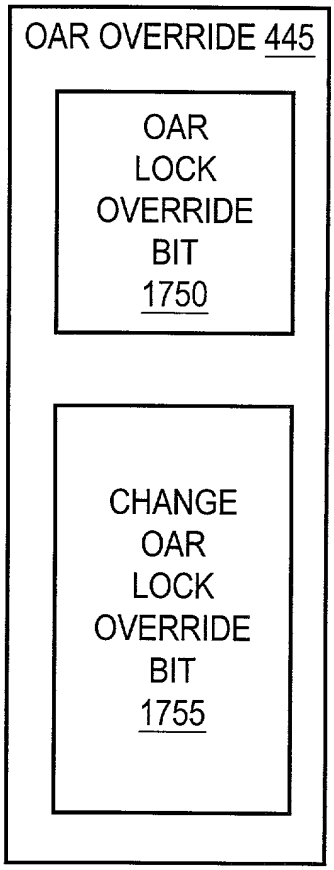

Fig. 17D

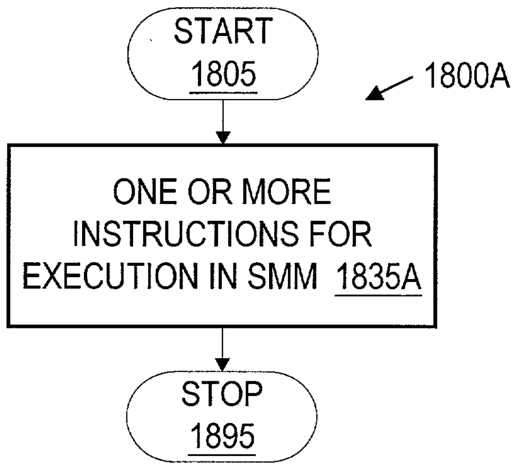

Fig. 18A
PRIOR ART

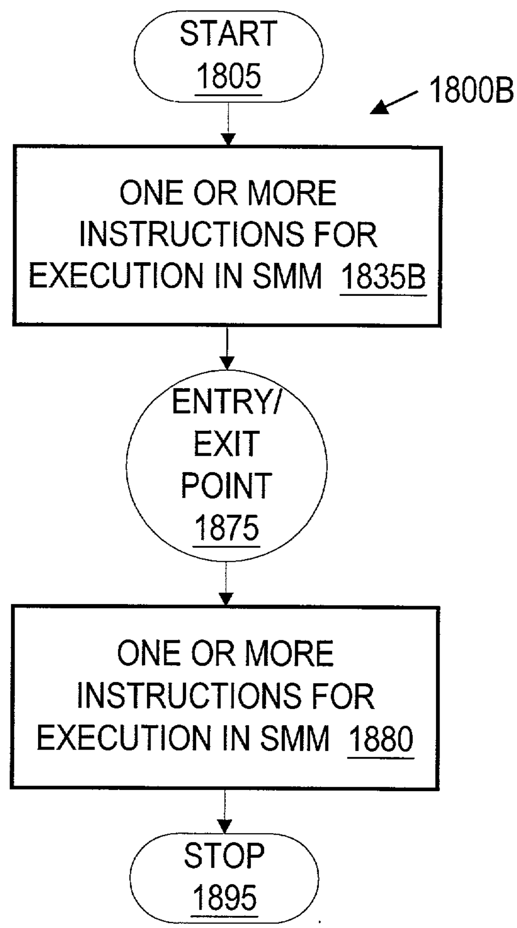

Fig. 18B

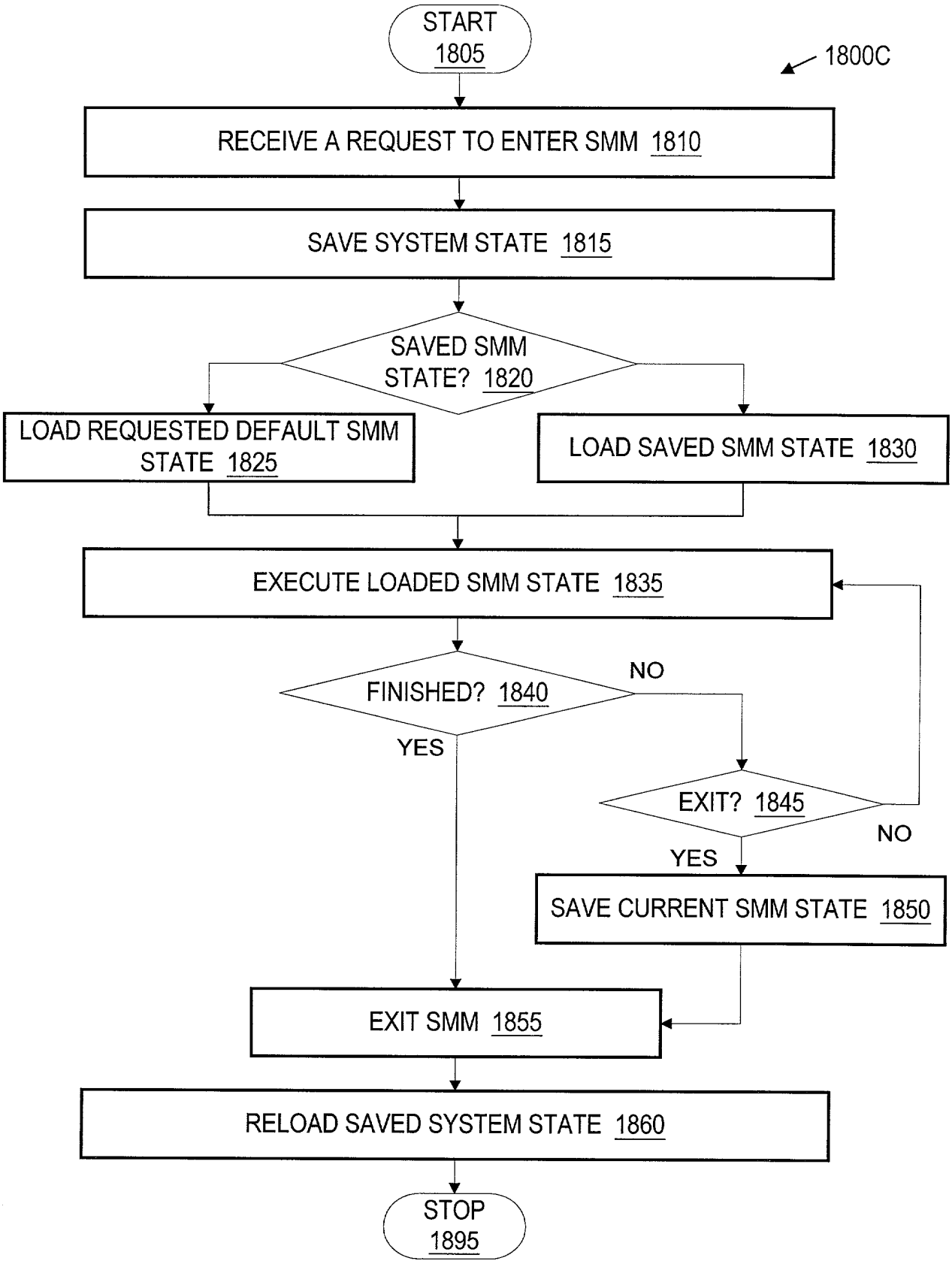

Fig. 18C

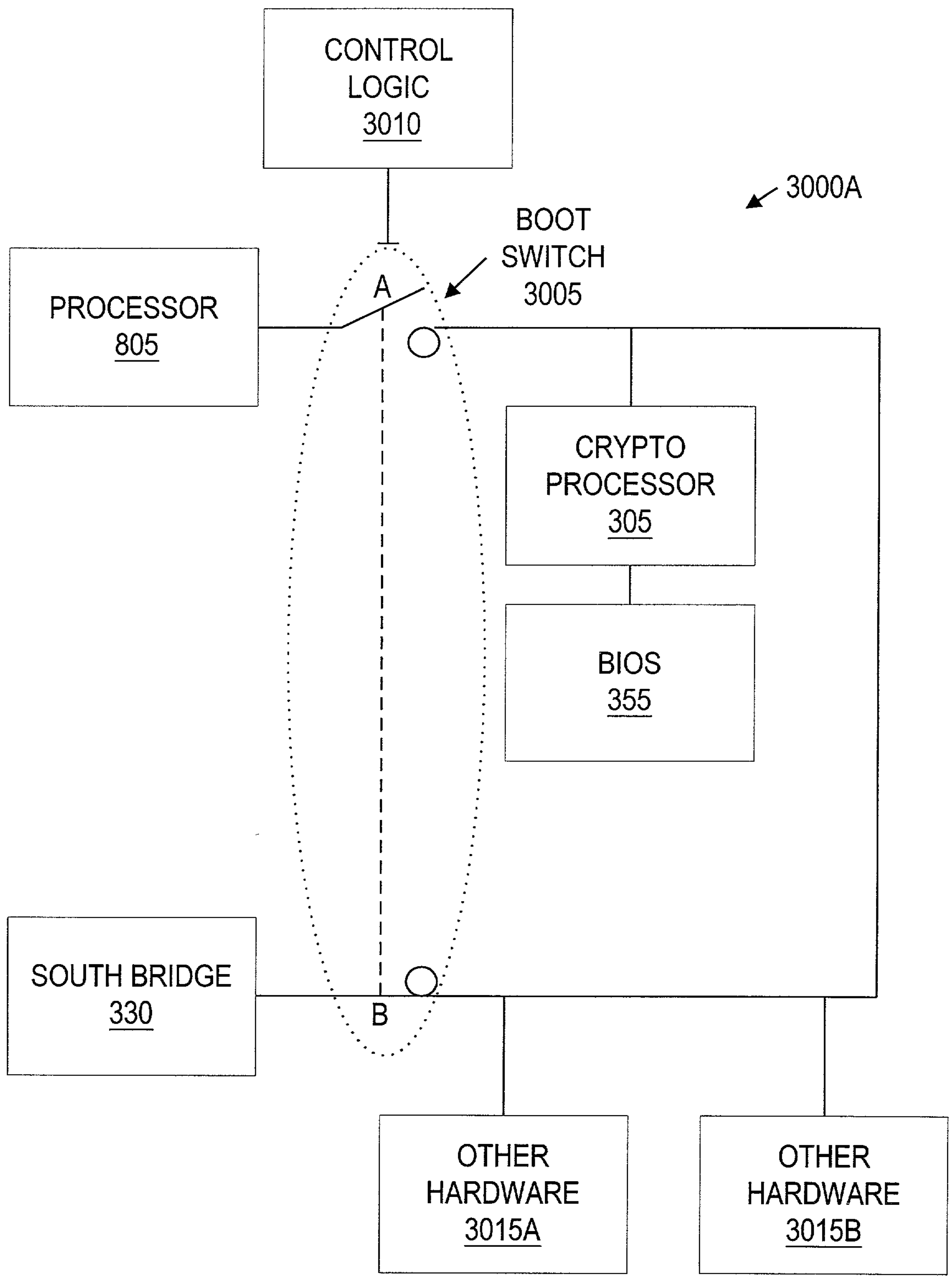

Fig. 19A

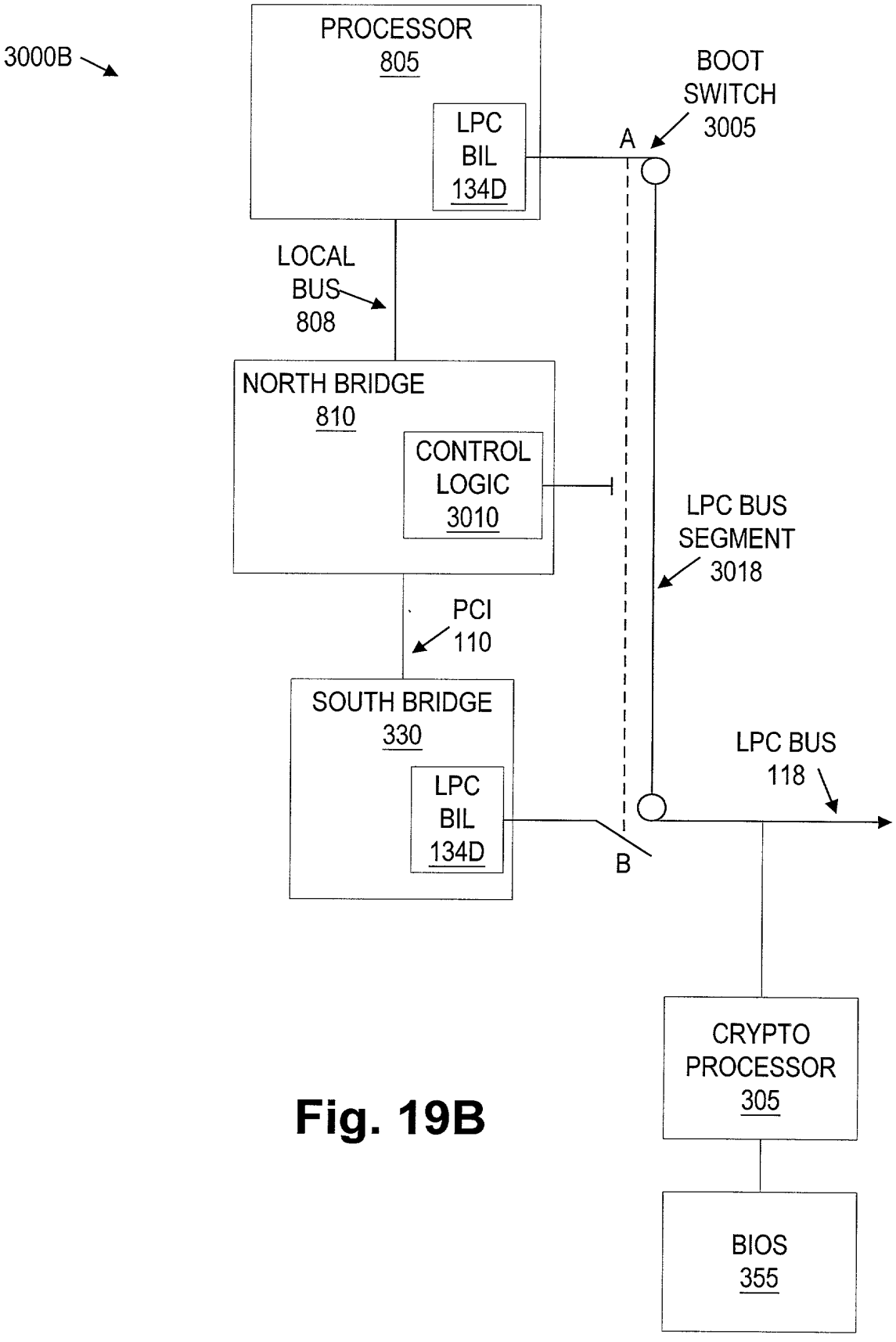

Fig. 19B

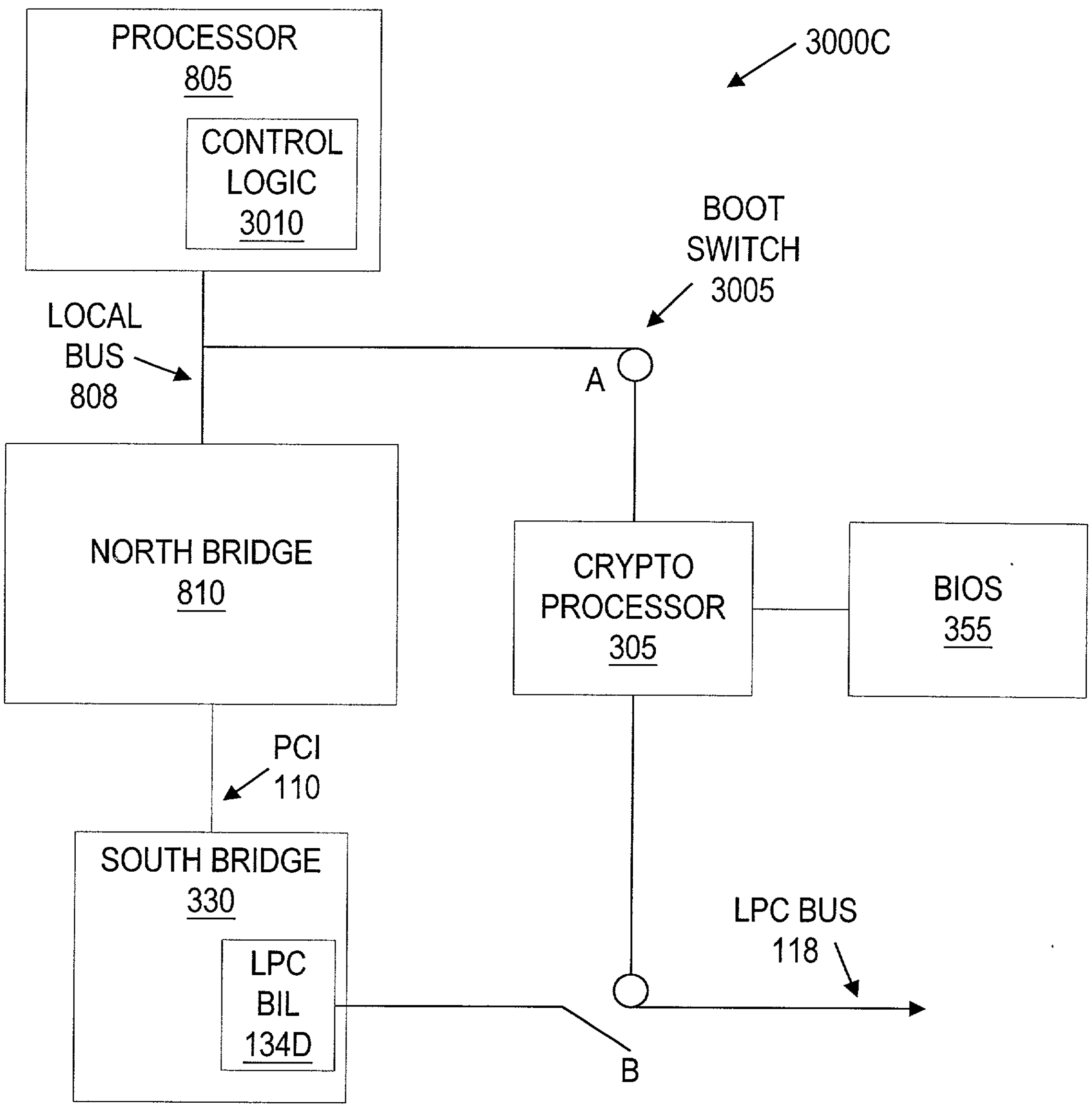

Fig. 19C

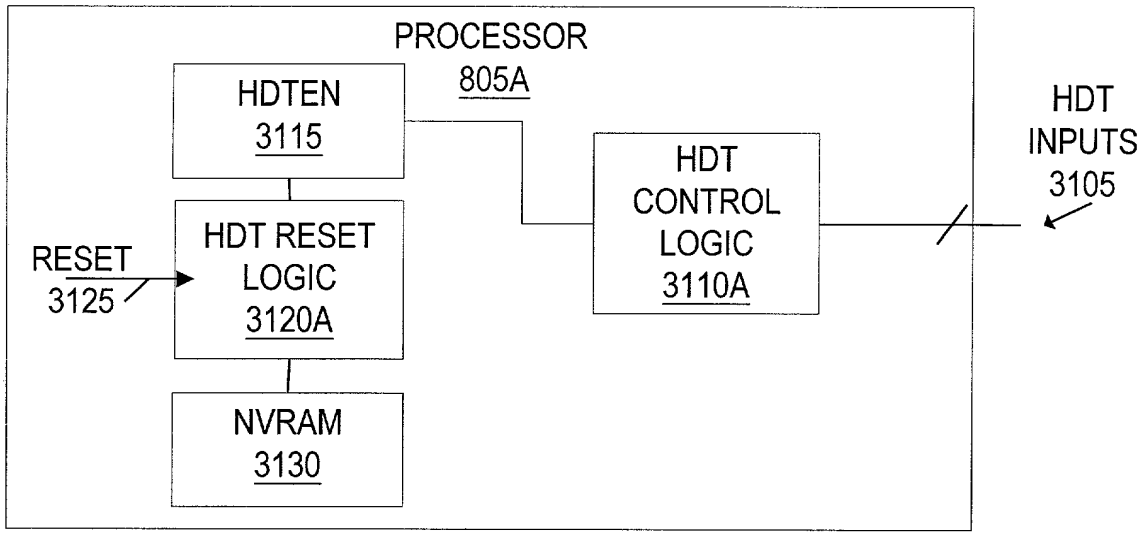

Fig. 20A

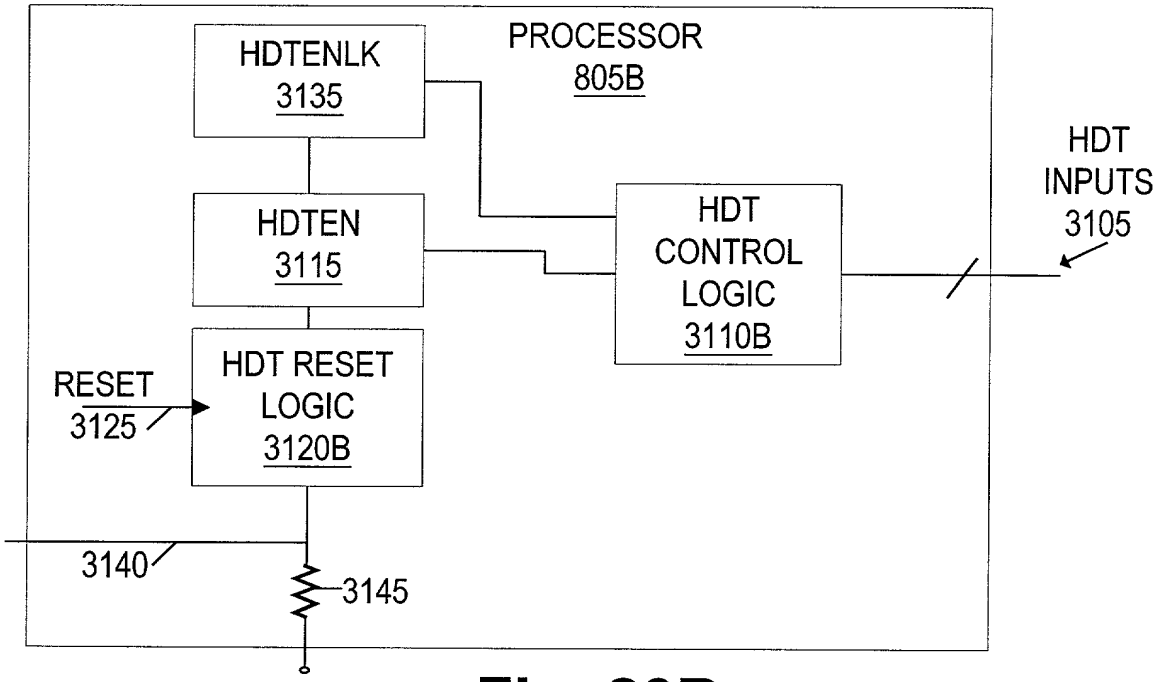

Fig. 20B

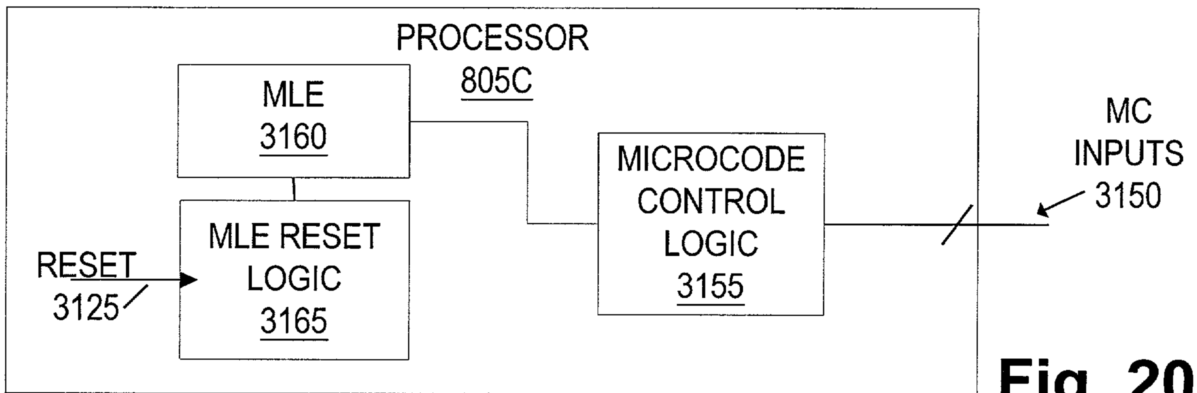

Fig. 20C

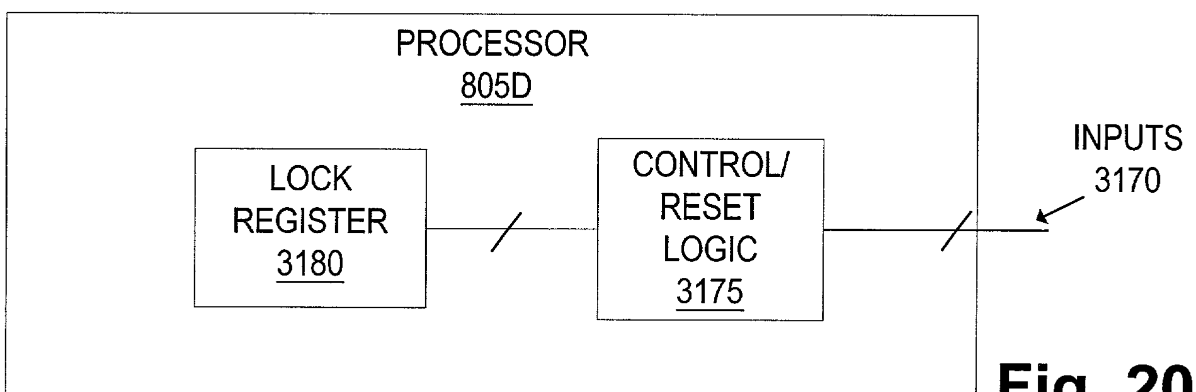

Fig. 20D

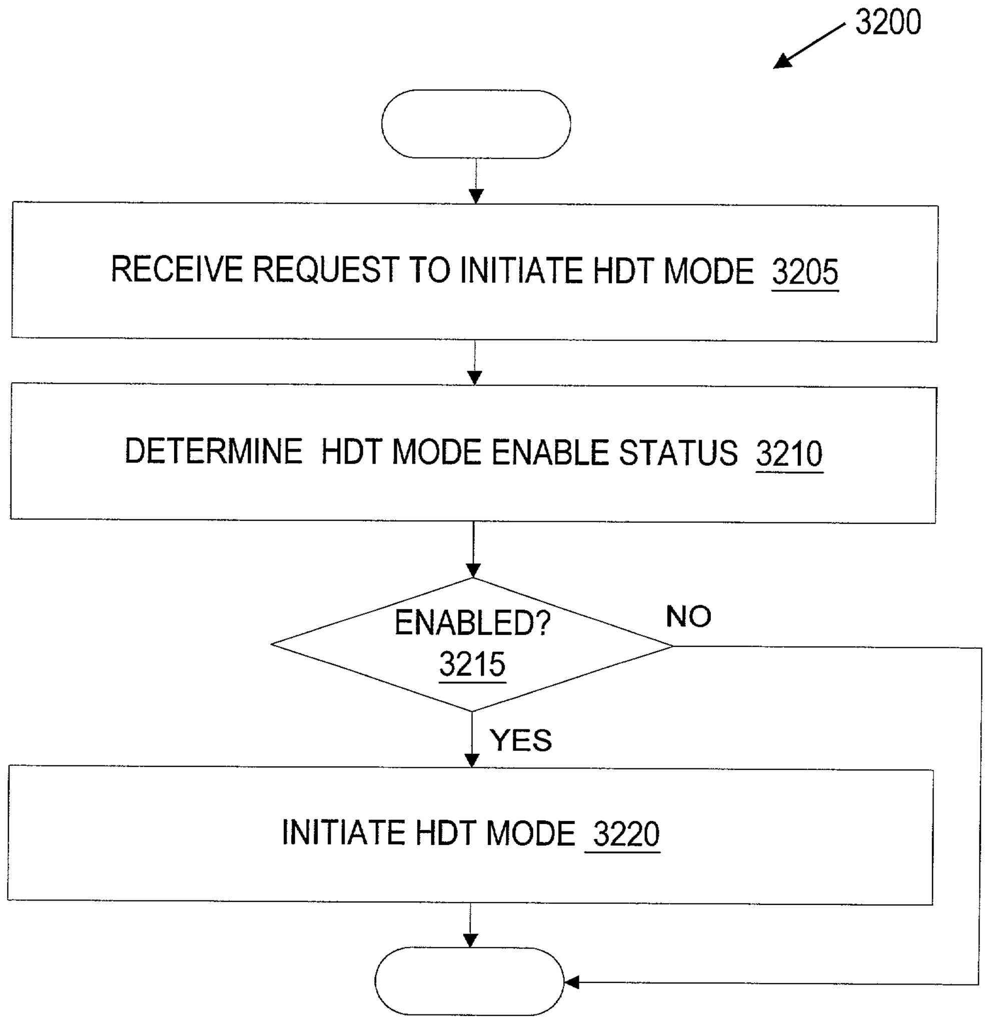

Fig. 21

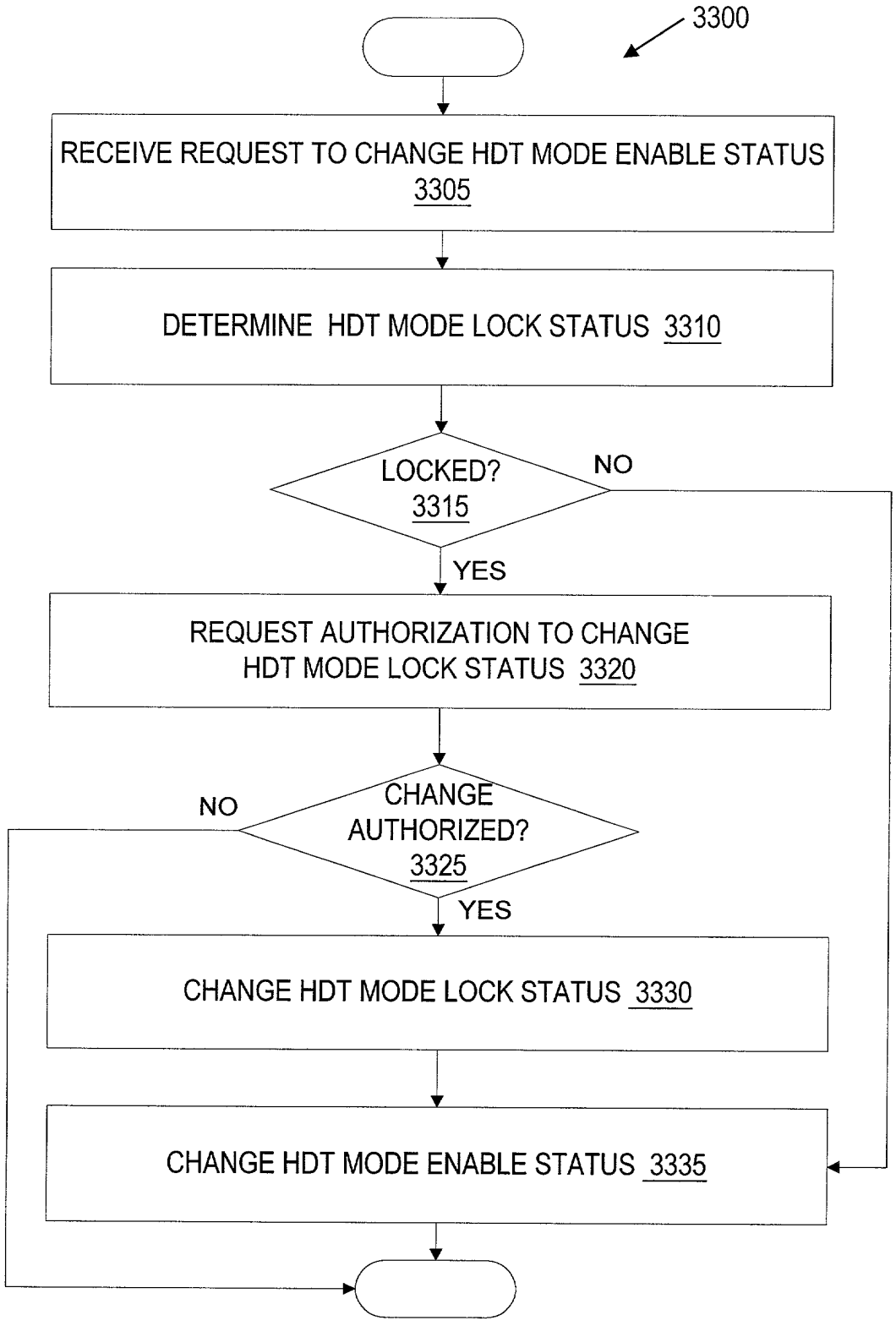
3300
RECEIVE REQUEST TO CHANGE HDT MODE ENABLE STATUS 3305
DETERMINE HDT MODE LOCK STATUS 3310
LOCKED? 3315
NO
YES
REQUEST AUTHORIZATION TO CHANGE HDT MODE LOCK STATUS 3320
CHANGE AUTHORIZED? 3325
NO
YES
CHANGE HDT MODE LOCK STATUS 3330
CHANGE HDT MODE ENABLE STATUS 3335

Fig. 22

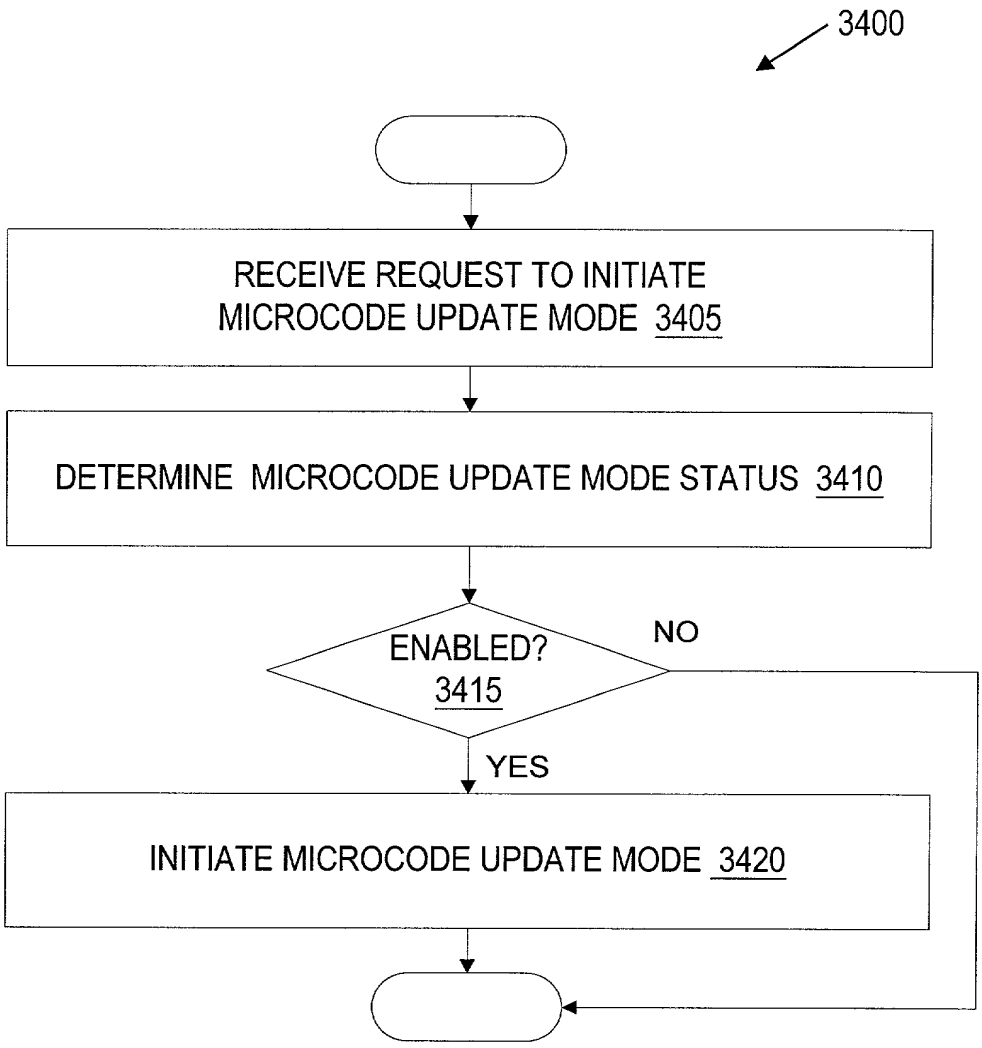

Fig. 23

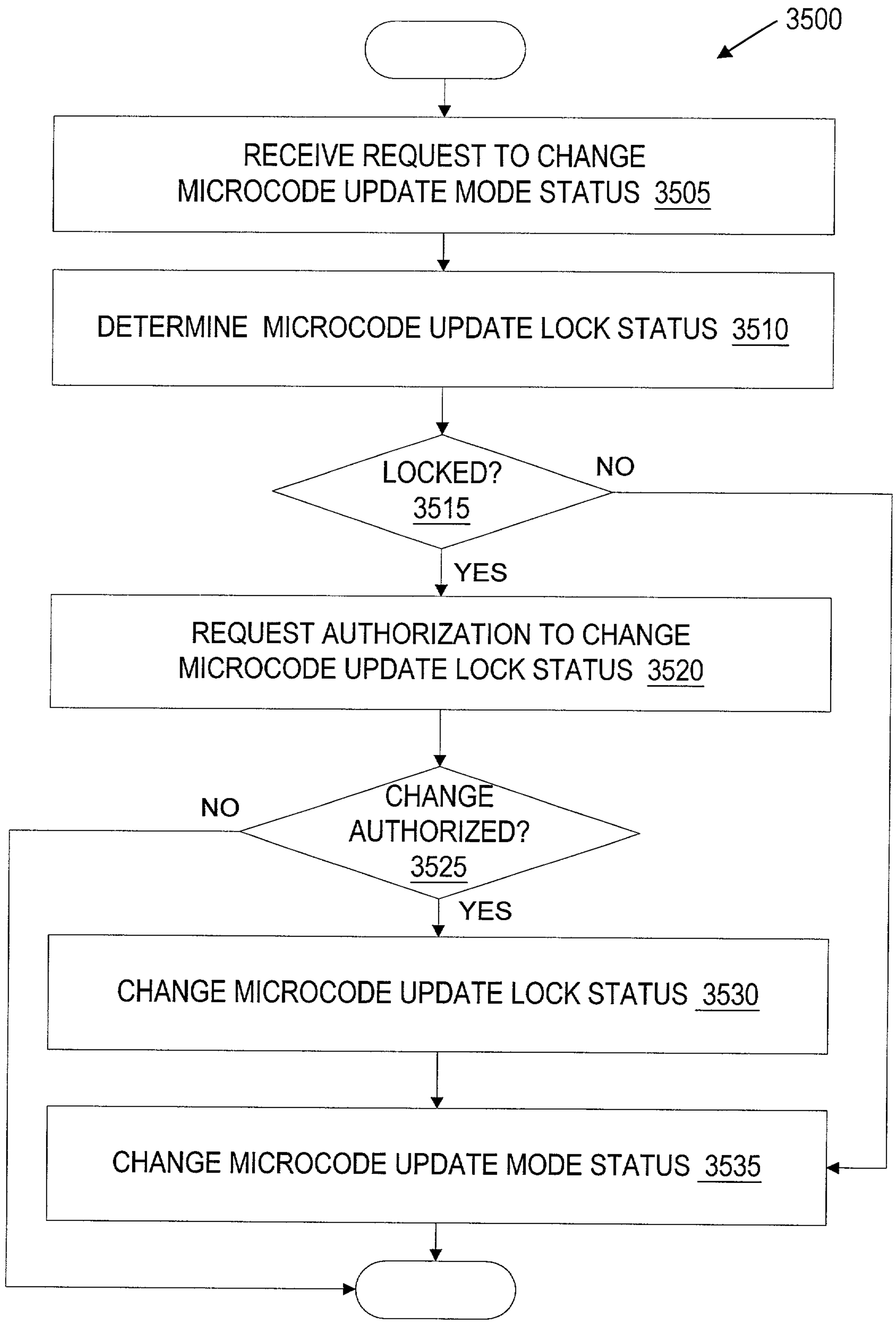

Fig. 24

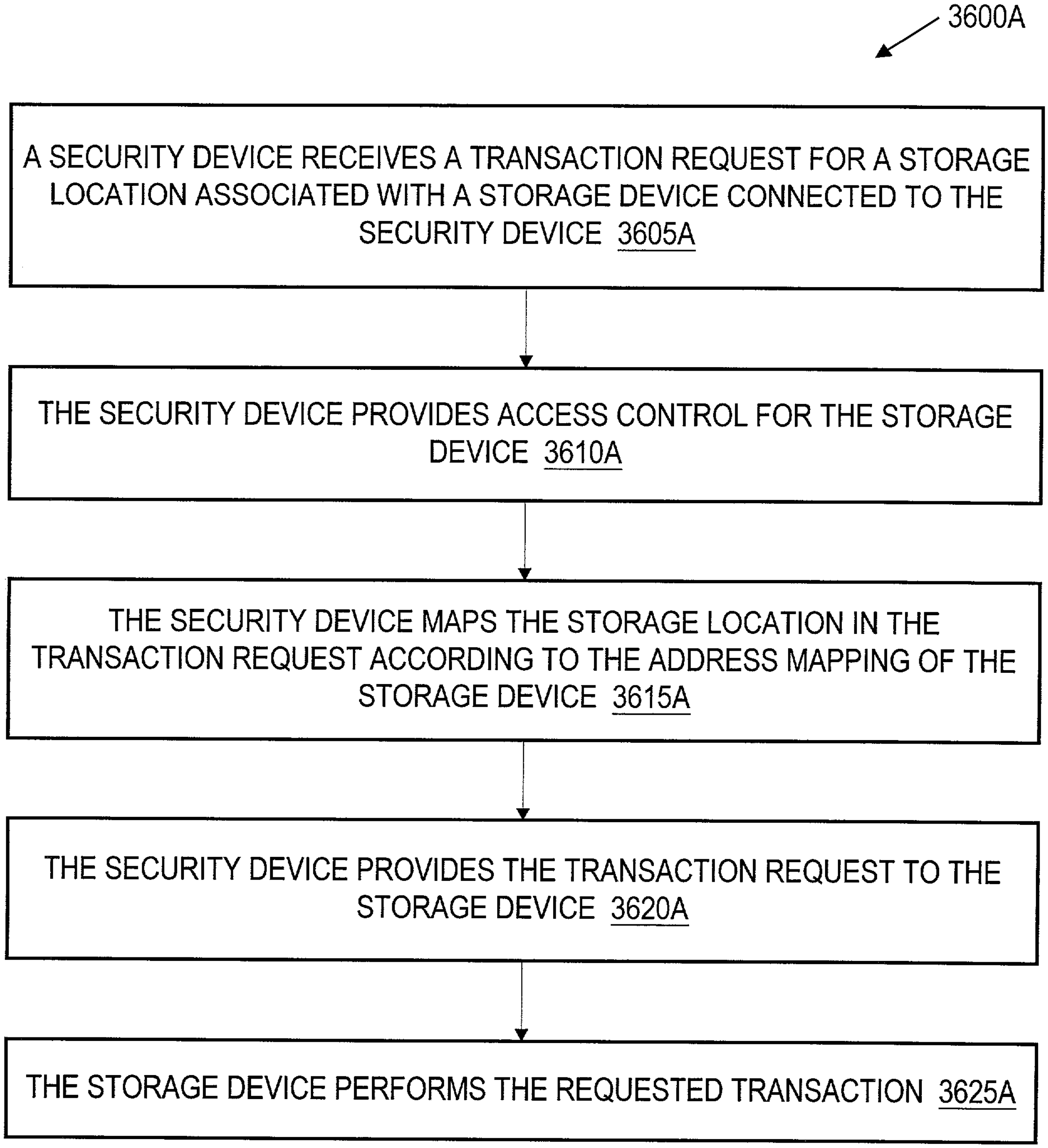

Fig. 25A

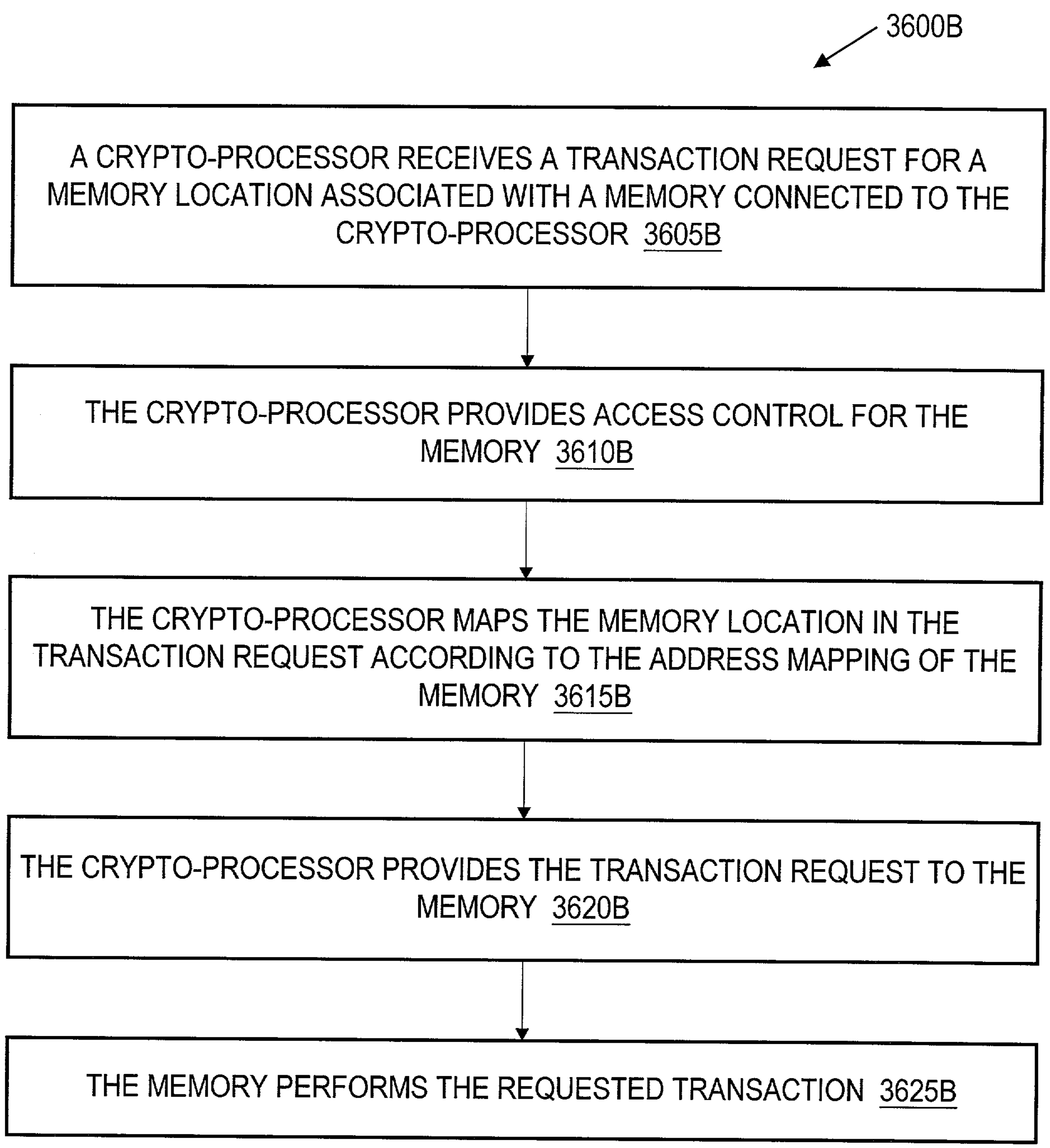

Fig. 25B

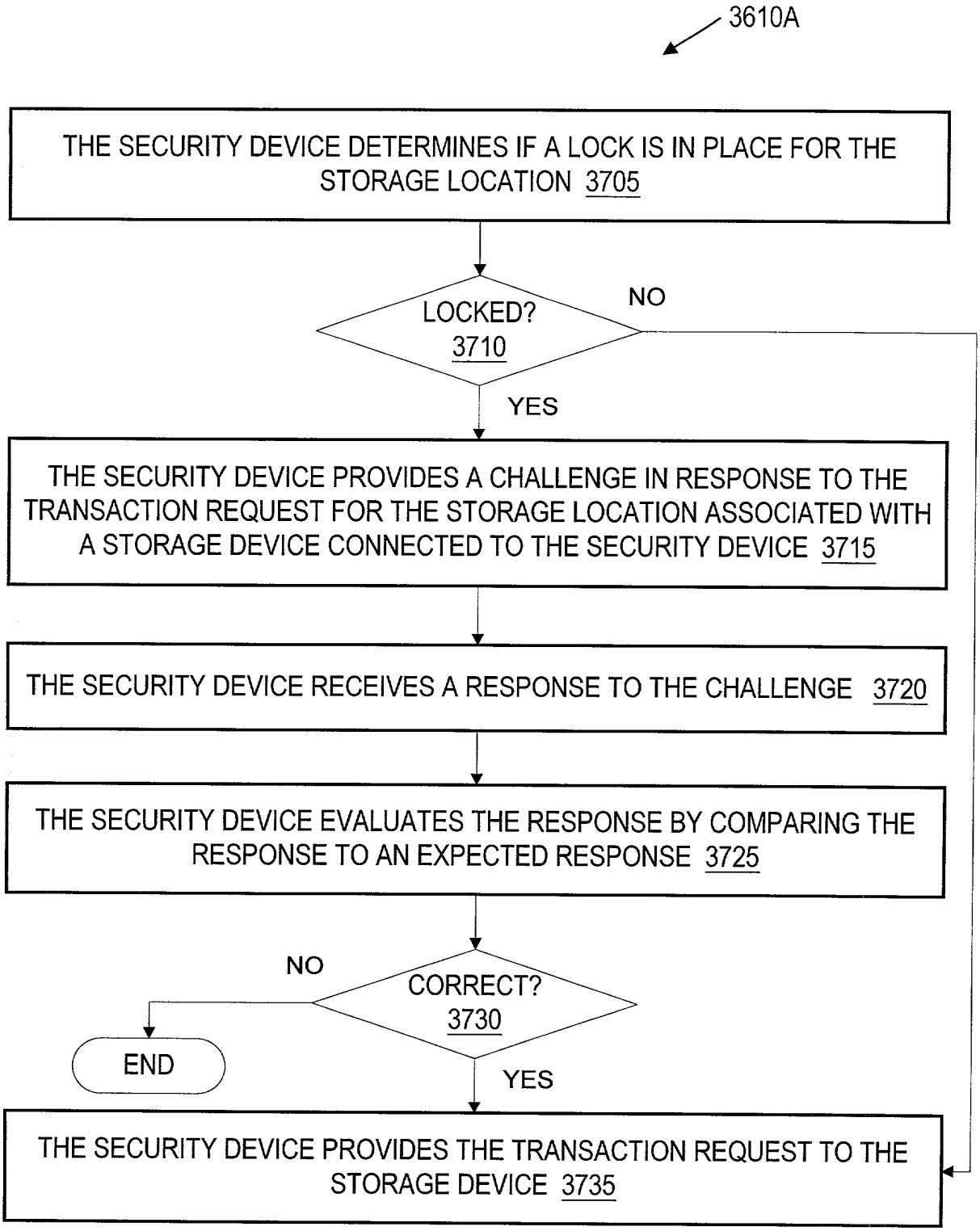
3610A
THE SECURITY DEVICE DETERMINES IF A LOCK IS IN PLACE FOR THE STORAGE LOCATION 3705
LOCKED? 3710
NO
YES
THE SECURITY DEVICE PROVIDES A CHALLENGE IN RESPONSE TO THE TRANSACTION REQUEST FOR THE STORAGE LOCATION ASSOCIATED WITH A STORAGE DEVICE CONNECTED TO THE SECURITY DEVICE 3715
THE SECURITY DEVICE RECEIVES A RESPONSE TO THE CHALLENGE 3720
THE SECURITY DEVICE EVALUATES THE RESPONSE BY COMPARING THE RESPONSE TO AN EXPECTED RESPONSE 3725
NO
CORRECT? 3730
END
YES
THE SECURITY DEVICE PROVIDES THE TRANSACTION REQUEST TO THE STORAGE DEVICE 3735

Fig. 26

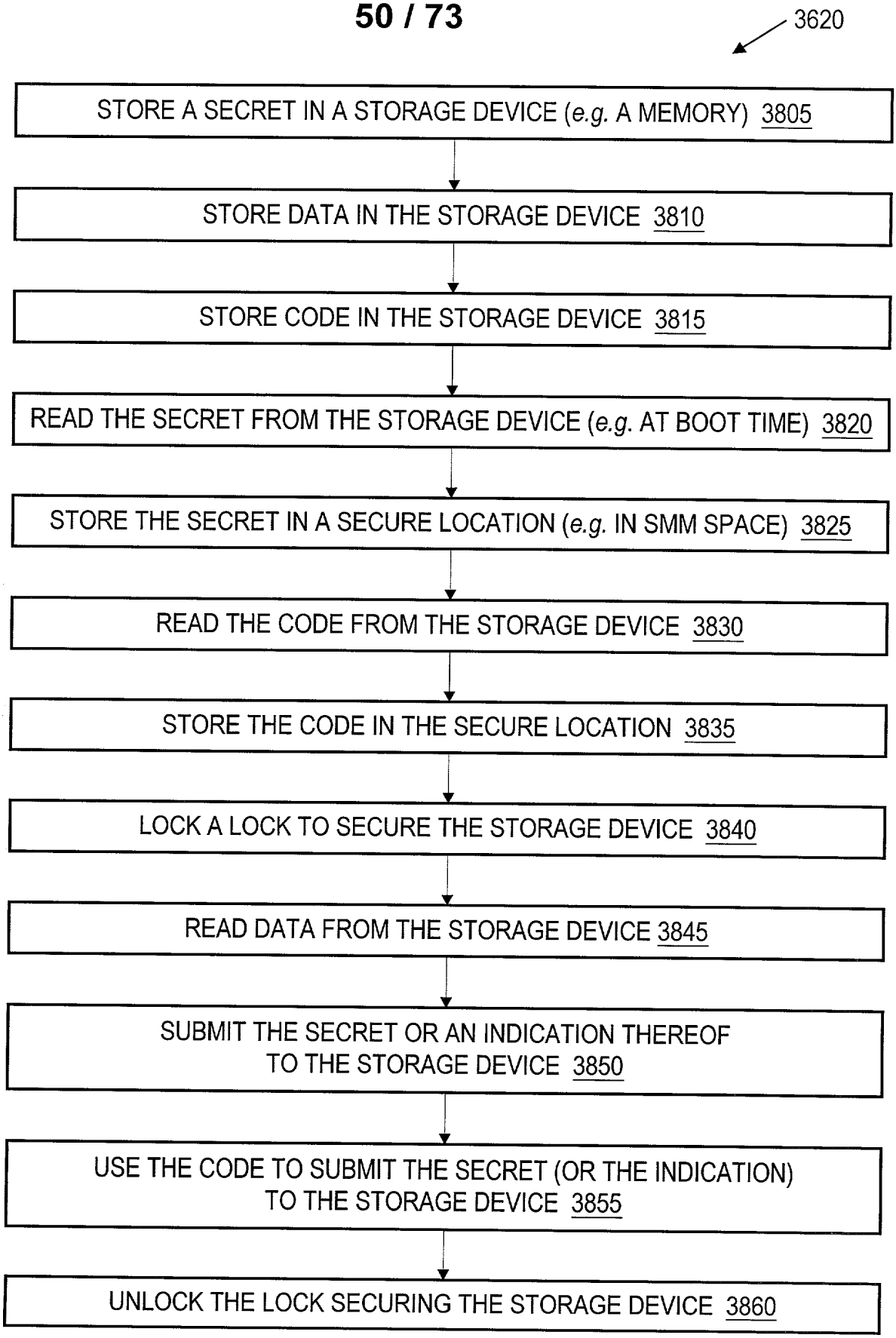

Fig. 27

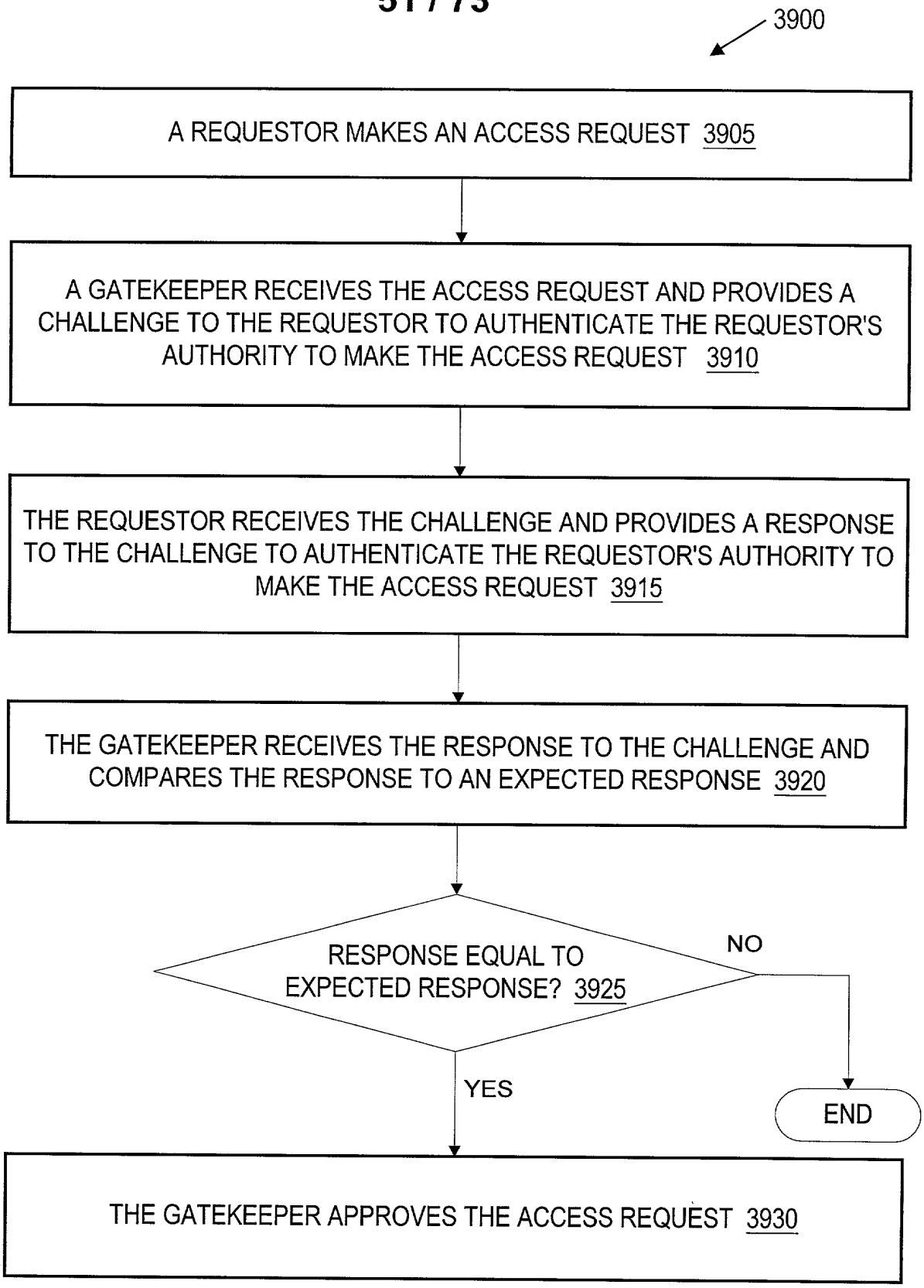

Fig. 28
(Prior Art)

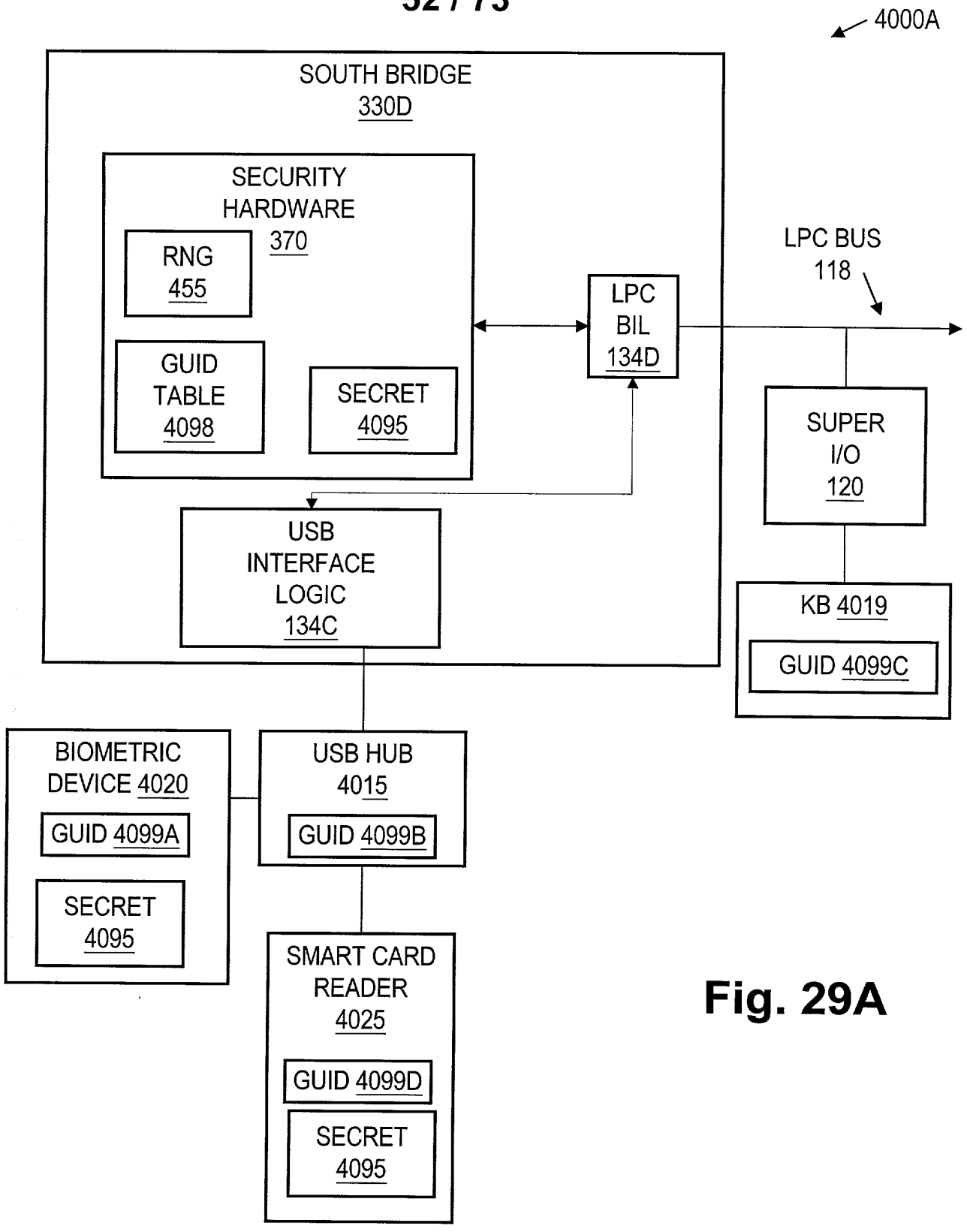

Fig. 29A

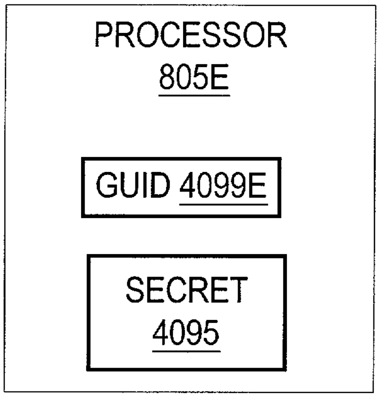

Fig. 29B

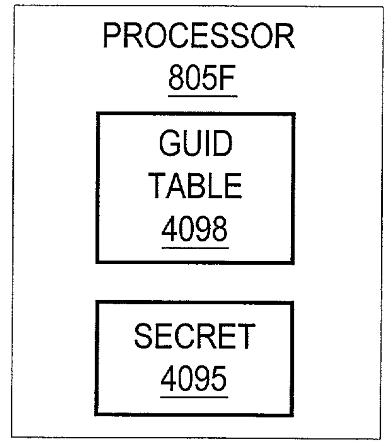

Fig. 29C

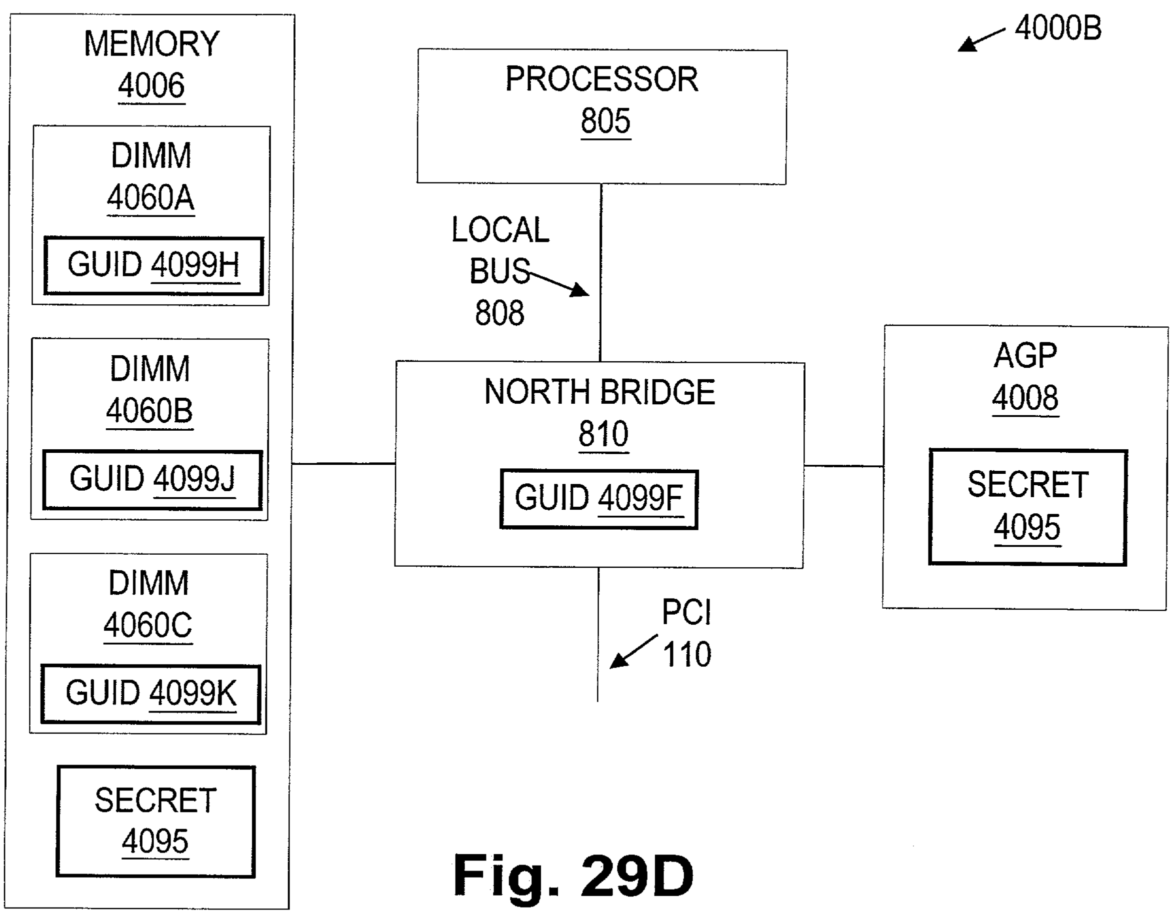

Fig. 29D

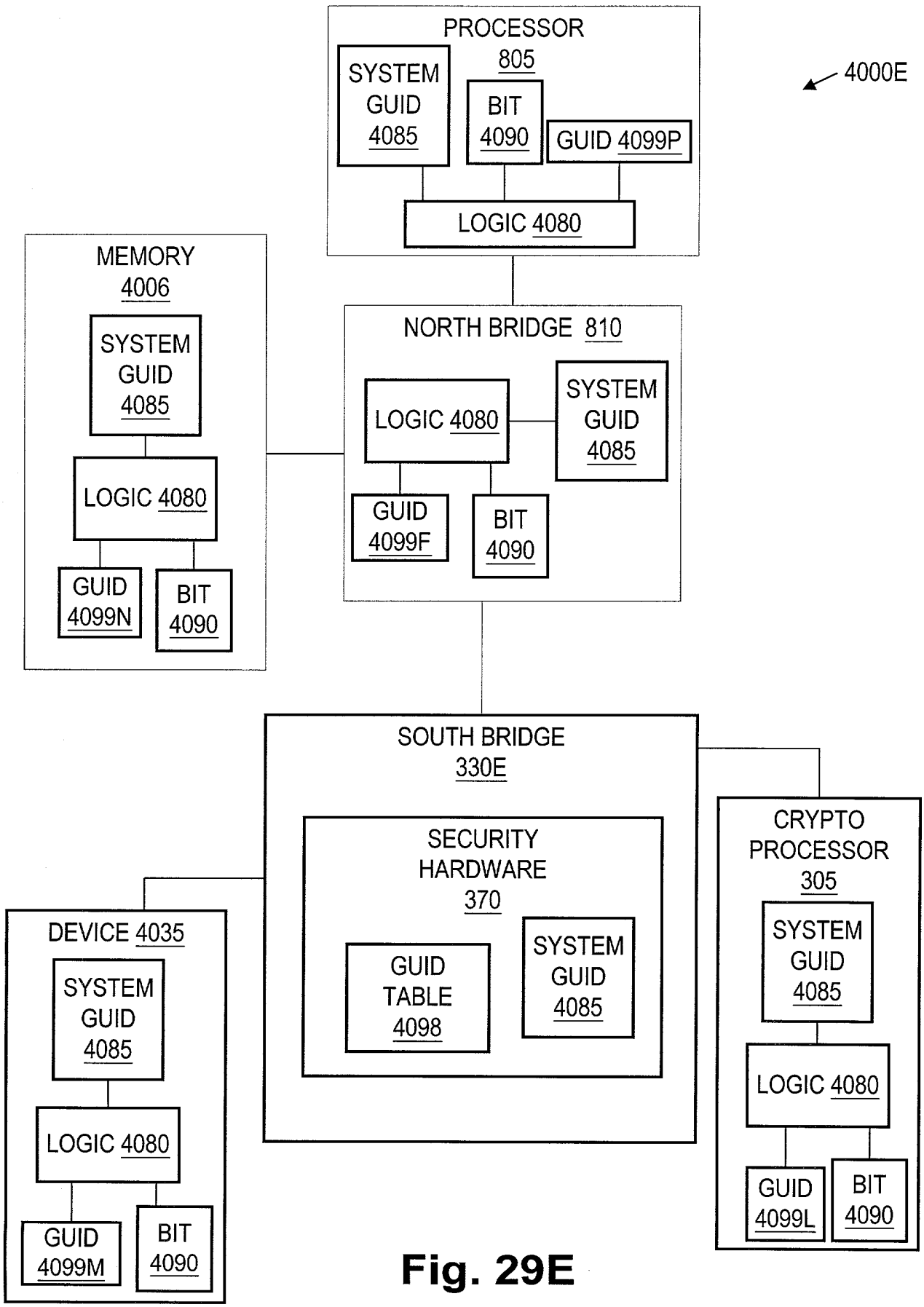

Fig. 29E

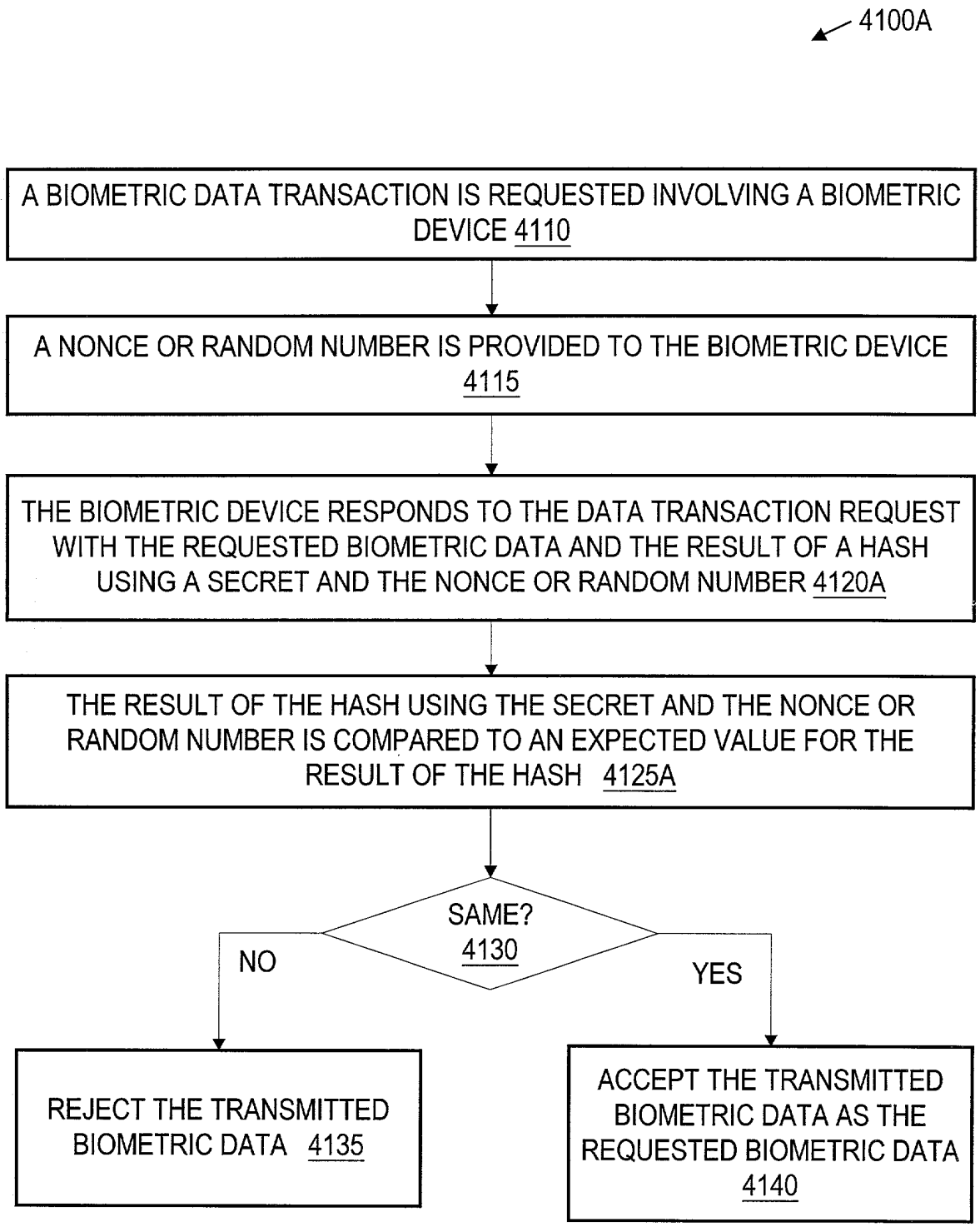
4100A
A BIOMETRIC DATA TRANSACTION IS REQUESTED INVOLVING A BIOMETRIC DEVICE 4110
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE BIOMETRIC DEVICE 4115
THE BIOMETRIC DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH THE REQUESTED BIOMETRIC DATA AND THE RESULT OF A HASH USING A SECRET AND THE NONCE OR RANDOM NUMBER 4120A
THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4125A
SAME? 4130
NO
YES
REJECT THE TRANSMITTED BIOMETRIC DATA 4135
ACCEPT THE TRANSMITTED BIOMETRIC DATA AS THE REQUESTED BIOMETRIC DATA 4140

Fig. 30A

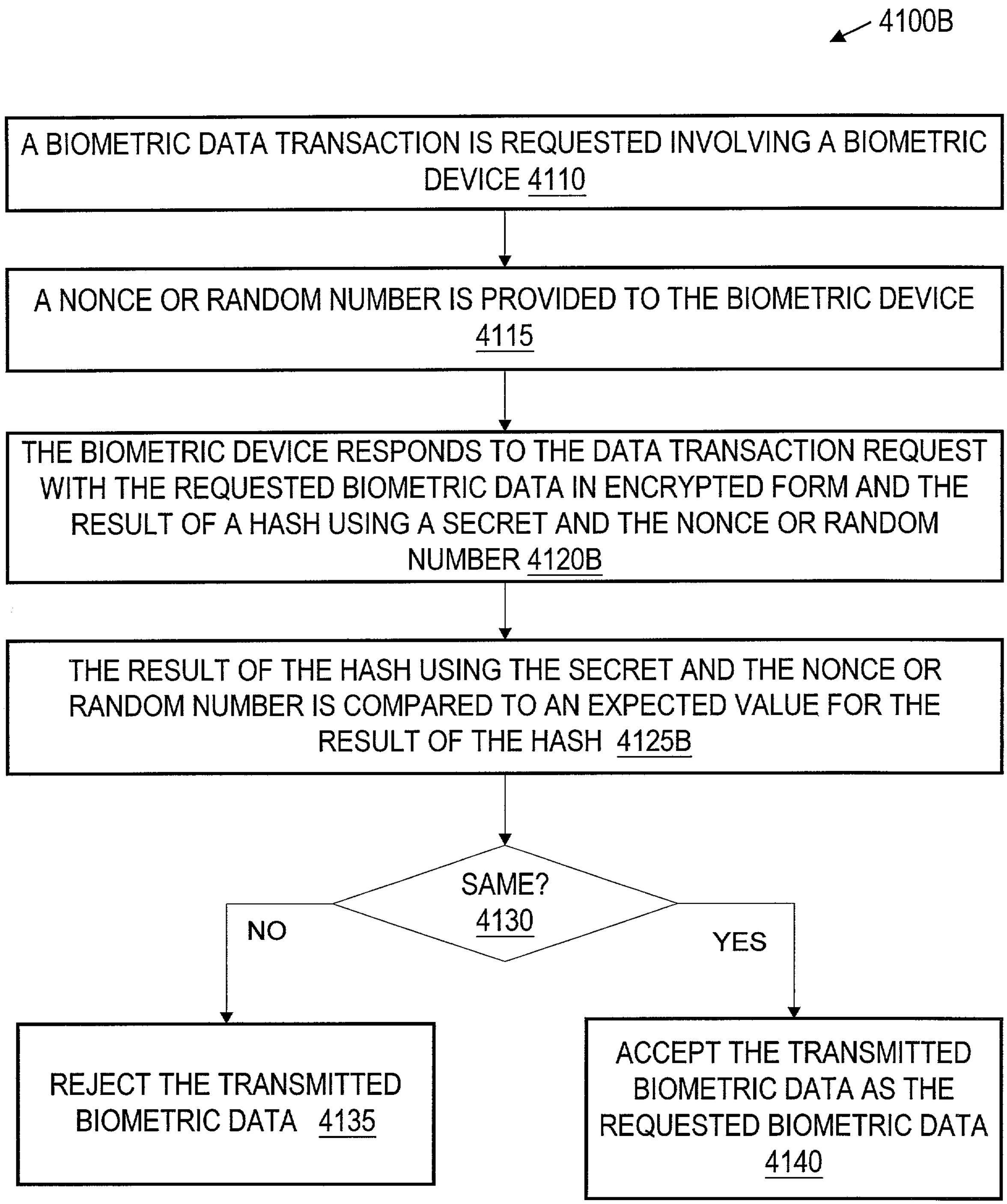
4100B
A BIOMETRIC DATA TRANSACTION IS REQUESTED INVOLVING A BIOMETRIC DEVICE 4110
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE BIOMETRIC DEVICE 4115
THE BIOMETRIC DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH THE REQUESTED BIOMETRIC DATA IN ENCRYPTED FORM AND THE RESULT OF A HASH USING A SECRET AND THE NONCE OR RANDOM NUMBER 4120B
THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4125B
SAME? 4130
NO
YES
REJECT THE TRANSMITTED BIOMETRIC DATA 4135
ACCEPT THE TRANSMITTED BIOMETRIC DATA AS THE REQUESTED BIOMETRIC DATA 4140

Fig. 30B

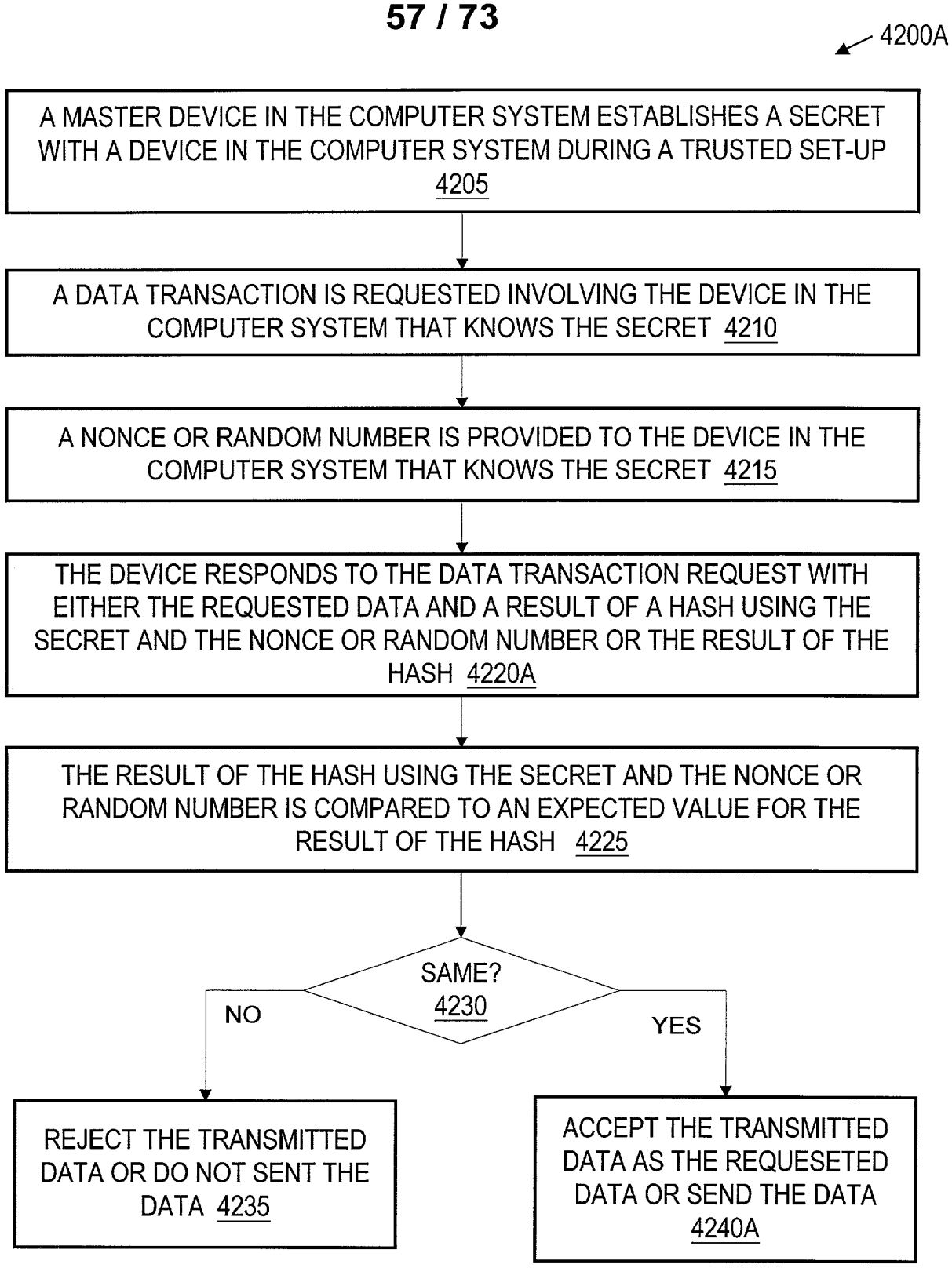
4200A
A MASTER DEVICE IN THE COMPUTER SYSTEM ESTABLISHES A SECRET WITH A DEVICE IN THE COMPUTER SYSTEM DURING A TRUSTED SET-UP 4205
A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM THAT KNOWS THE SECRET 4210
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM THAT KNOWS THE SECRET 4215
THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST WITH EITHER THE REQUESTED DATA AND A RESULT OF A HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER OR THE RESULT OF THE HASH 4220A
THE RESULT OF THE HASH USING THE SECRET AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4225
SAME? 4230
NO
YES
REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA 4235
ACCEPT THE TRANSMITTED DATA AS THE REQUESETED DATA OR SEND THE DATA 4240A

Fig. 31A

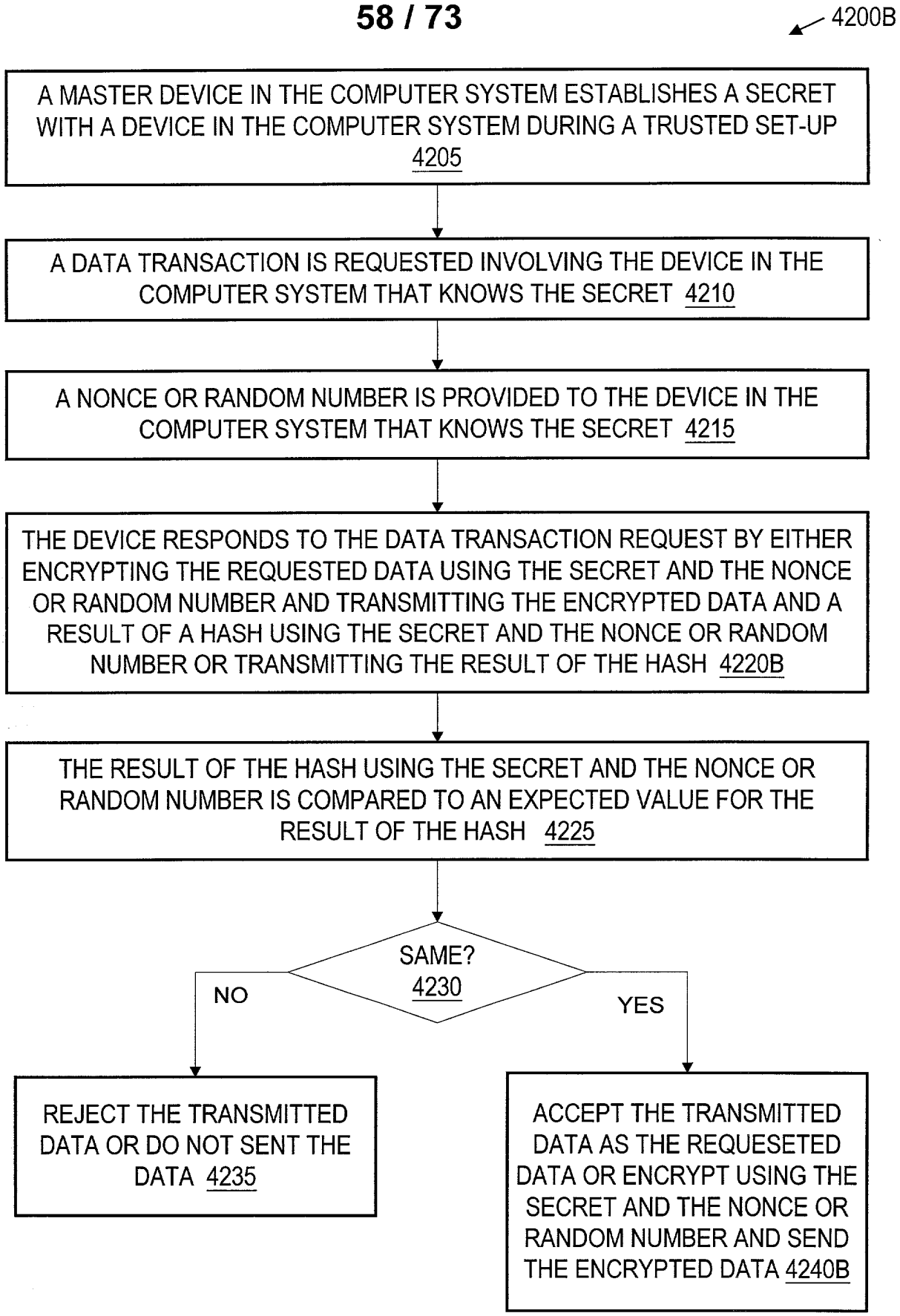

Fig. 31B

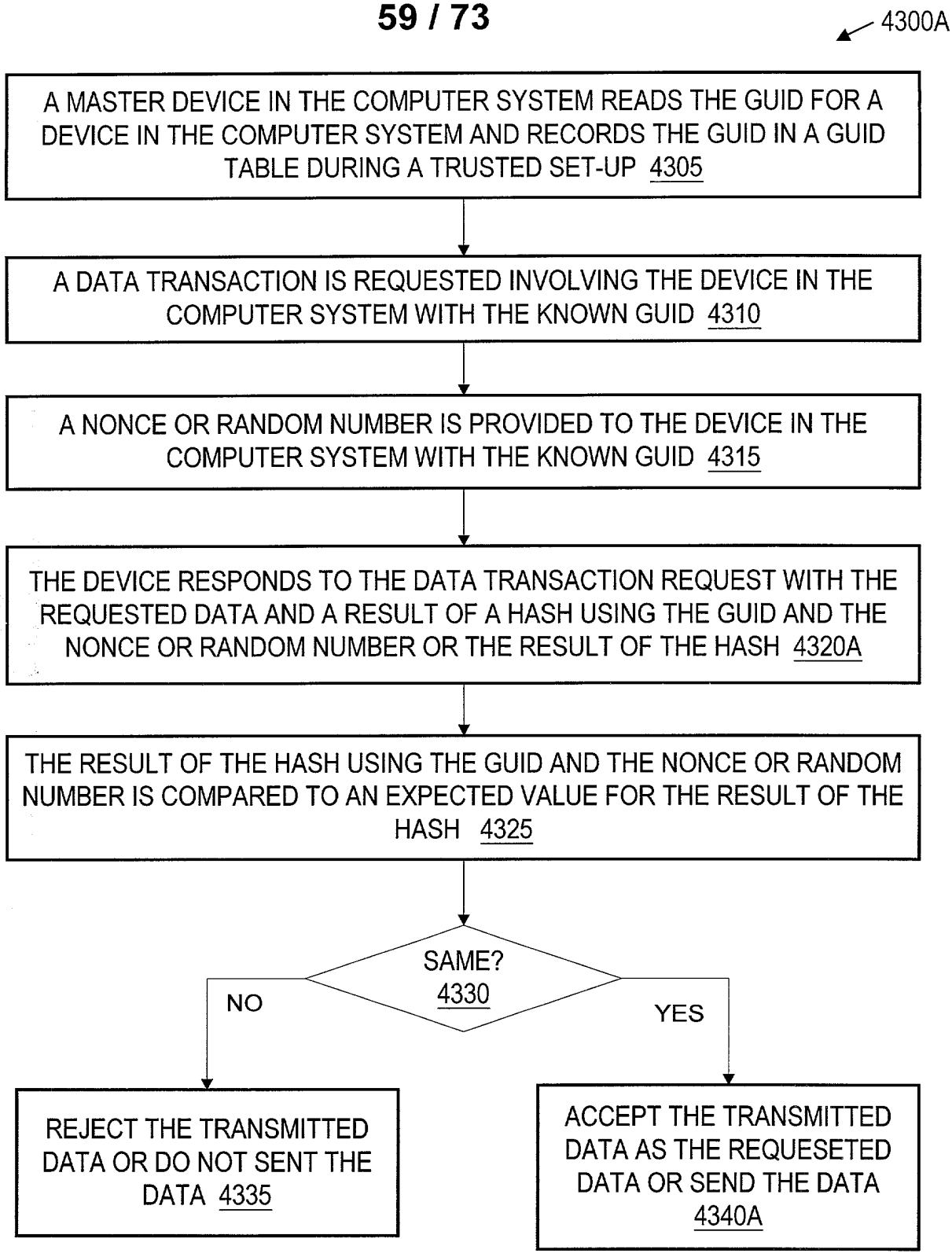

Fig. 32A

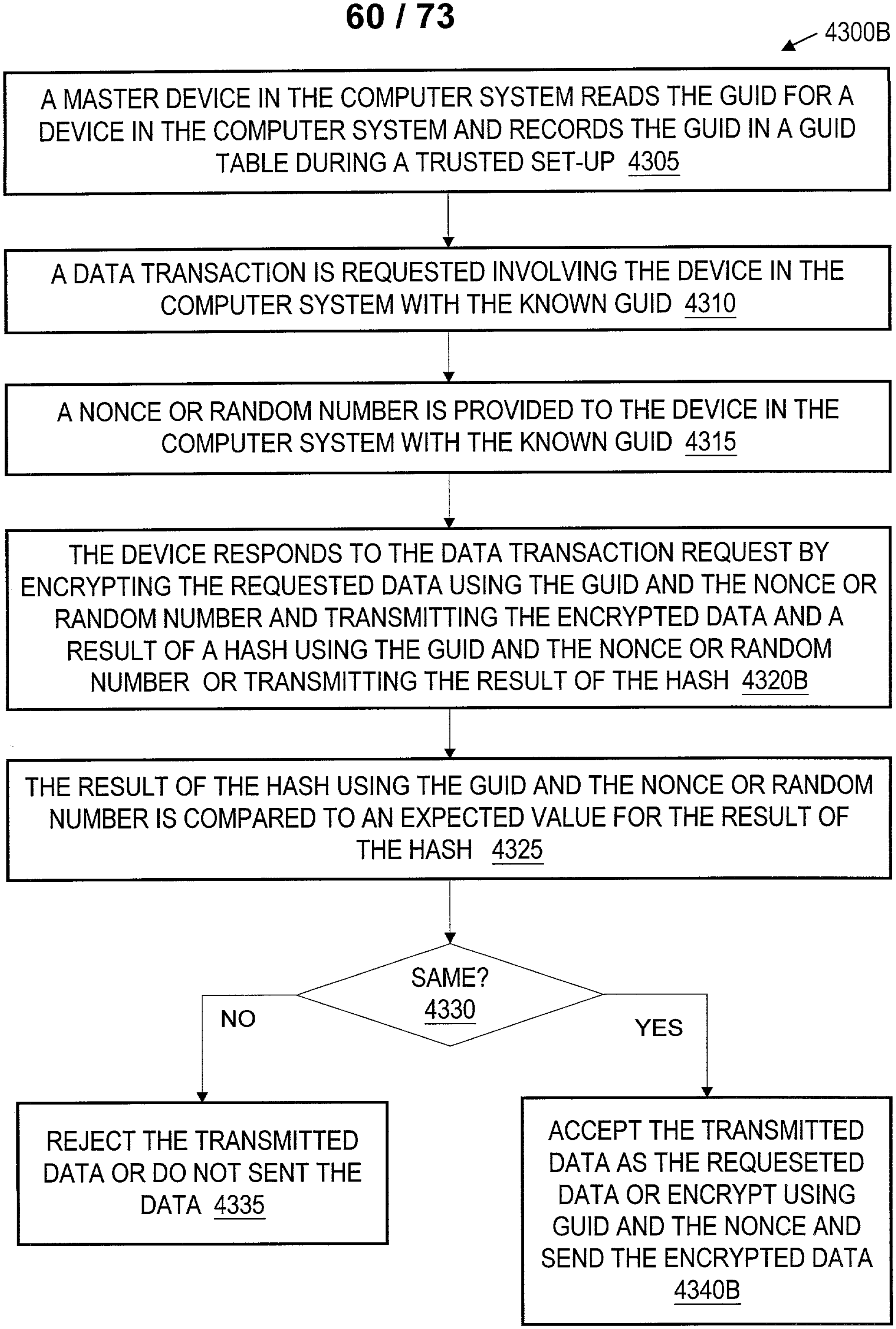
4300B
A MASTER DEVICE IN THE COMPUTER SYSTEM READS THE GUID FOR A DEVICE IN THE COMPUTER SYSTEM AND RECORDS THE GUID IN A GUID TABLE DURING A TRUSTED SET-UP 4305
A DATA TRANSACTION IS REQUESTED INVOLVING THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID 4310
A NONCE OR RANDOM NUMBER IS PROVIDED TO THE DEVICE IN THE COMPUTER SYSTEM WITH THE KNOWN GUID 4315
THE DEVICE RESPONDS TO THE DATA TRANSACTION REQUEST BY ENCRYPTING THE REQUESTED DATA USING THE GUID AND THE NONCE OR RANDOM NUMBER AND TRANSMITTING THE ENCRYPTED DATA AND A RESULT OF A HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER OR TRANSMITTING THE RESULT OF THE HASH 4320B
THE RESULT OF THE HASH USING THE GUID AND THE NONCE OR RANDOM NUMBER IS COMPARED TO AN EXPECTED VALUE FOR THE RESULT OF THE HASH 4325
SAME? 4330
NO
YES
REJECT THE TRANSMITTED DATA OR DO NOT SENT THE DATA 4335
ACCEPT THE TRANSMITTED DATA AS THE REQUESETED DATA OR ENCRYPT USING GUID AND THE NONCE AND SEND THE ENCRYPTED DATA 4340B

Fig. 32B

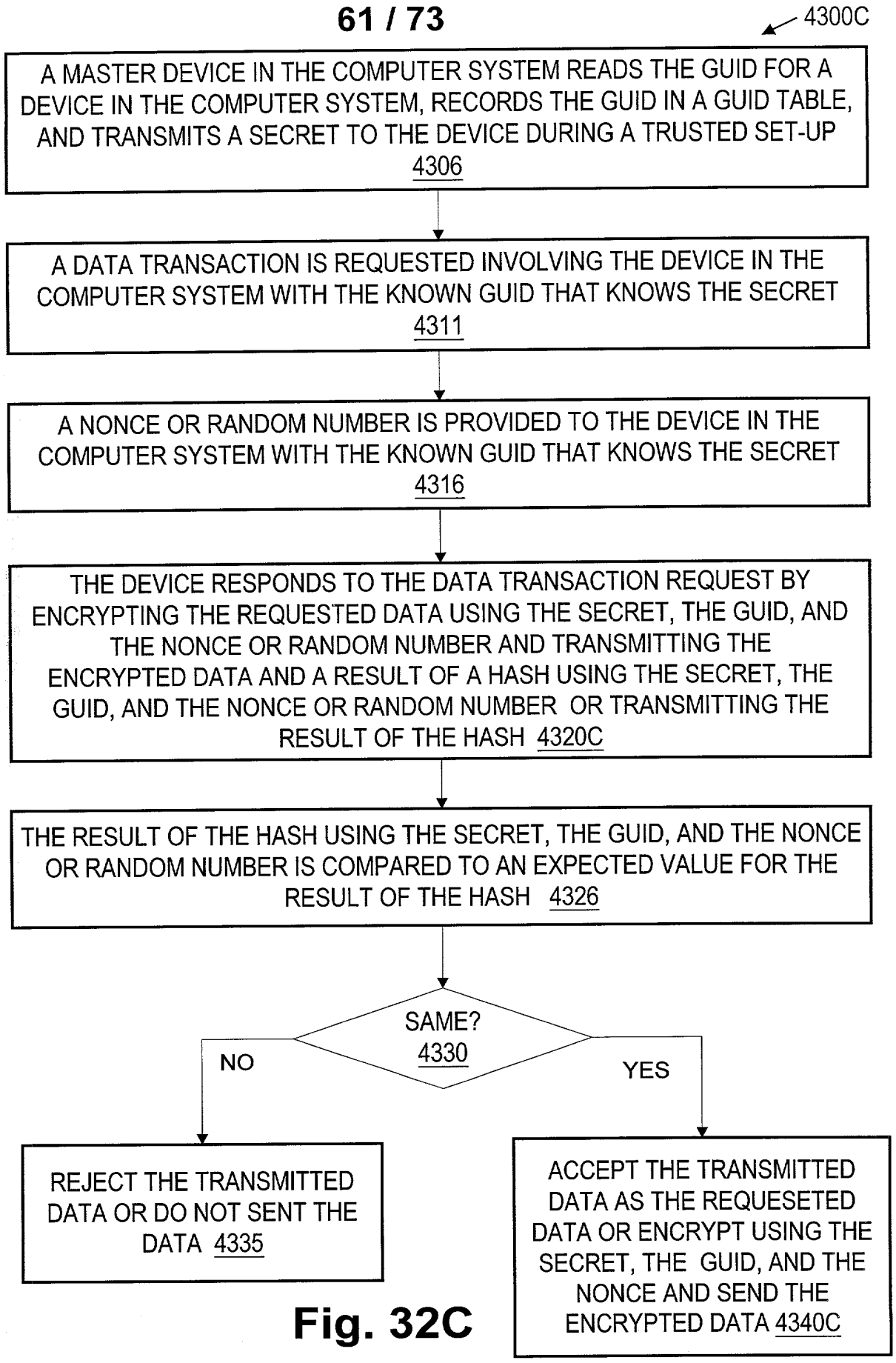

Fig. 32C

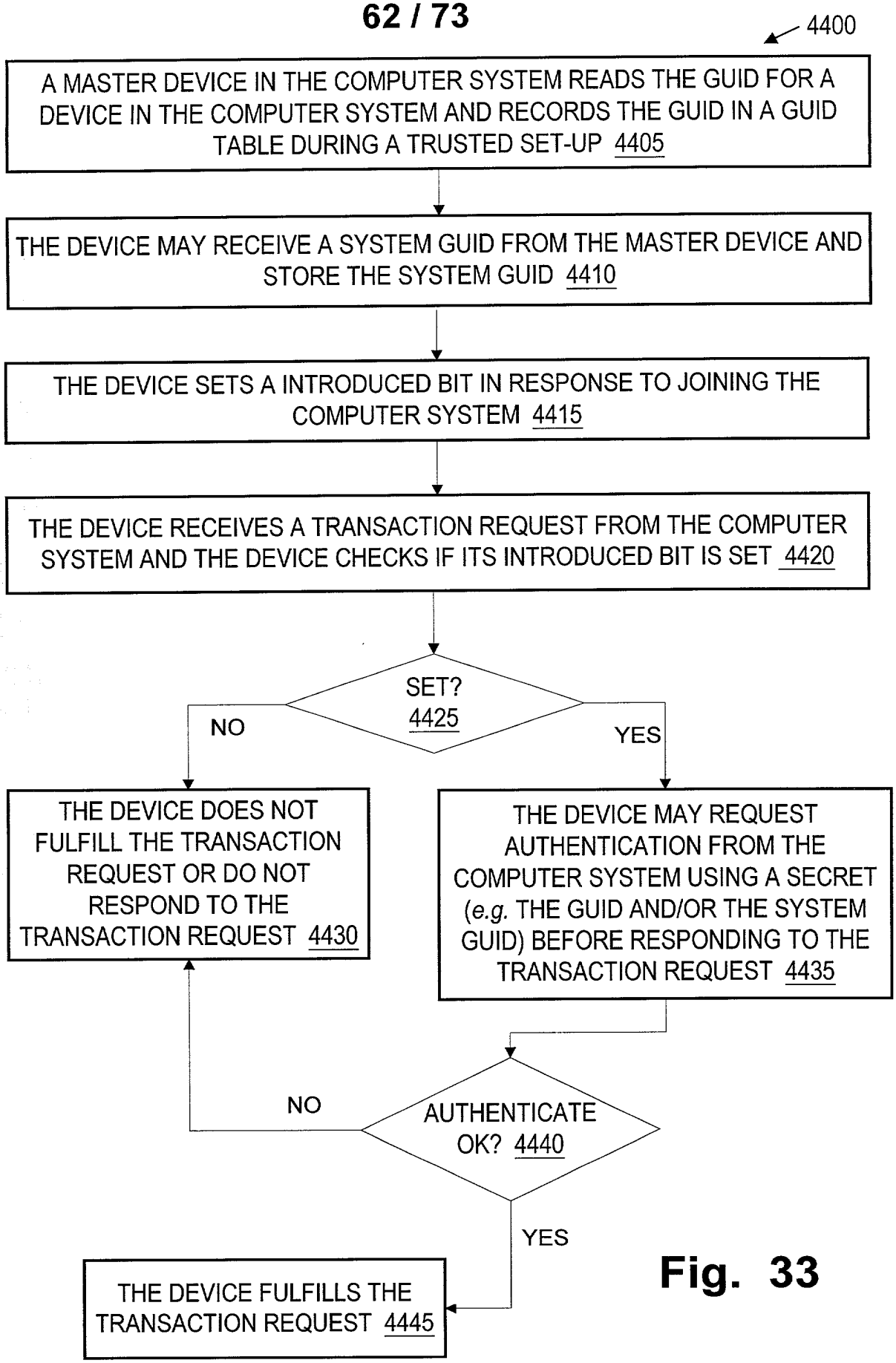

Fig. 33

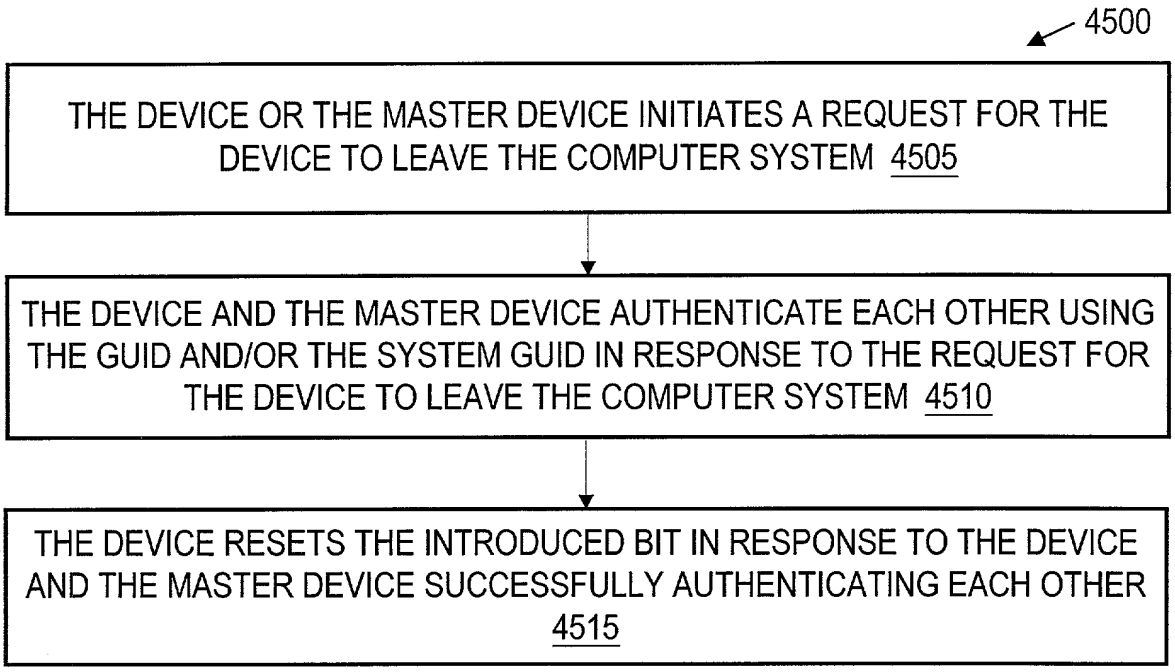

Fig. 34

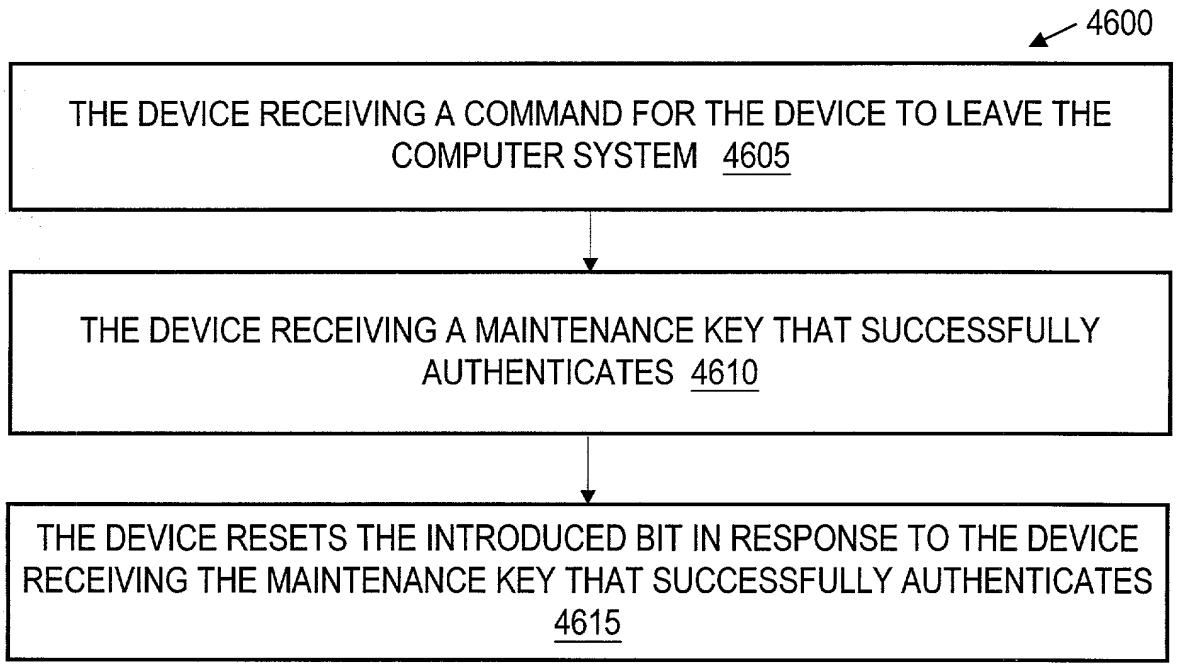

Fig. 35

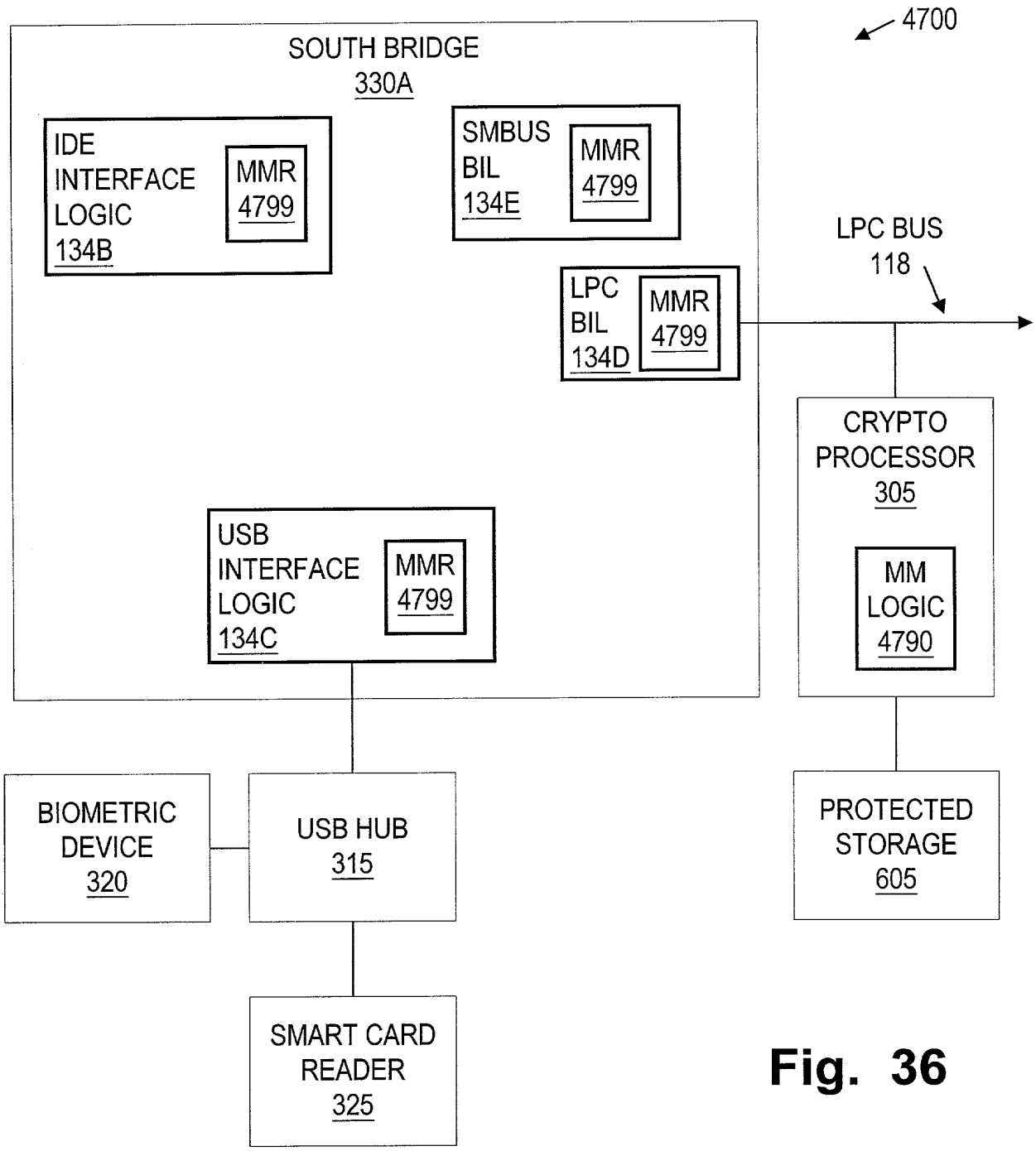

Fig. 36

4800

TRANSMIT A MASTER MODE SIGNAL TO BUS INTERFACE LOGIC CONNECTED BETWEEN MASTER MODE LOGIC AND A DATA INPUT DEVICE, WHERE THE BUS INTERFACE LOGIC INCLUDES A MASTER MODE REGISTER 4805

SET A MASTER MODE BIT IN THE MASTER MODE REGISTER(S) TO ESTABLISH SECURE TRANSMISSION CHANNEL BETWEEN THE MASTER MODE LOGIC AND THE DATA INPUT DEVICE OUTSIDE THE OPERATING SYSTEM OF THE COMPUTER SYSTEM 4810

THE MASTER MODE LOGIC AND THE DATA INPUT DEVICE EXCHANGE DATA OUTSIDE THE OPERATING SYSTEM OF THE COMPUTER SYSTEM THROUGH THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER 4815

THE MASTER MODE LOGIC FLUSHES THE BUFFERS OF THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER AFTER CONCLUDING THE DATA TRANSMISSIONS 4820

THE MASTER MODE LOGIC SIGNALS THE BUS INTERFACE LOGIC(S) TO UNSET THE MASER MODE BITS AFTER FLUSHING THE BUFFERS OF THE BUS INTERFACE LOGIC(S) THAT INCLUDE THE MASTER MODE REGISTER 4825

Fig. 37

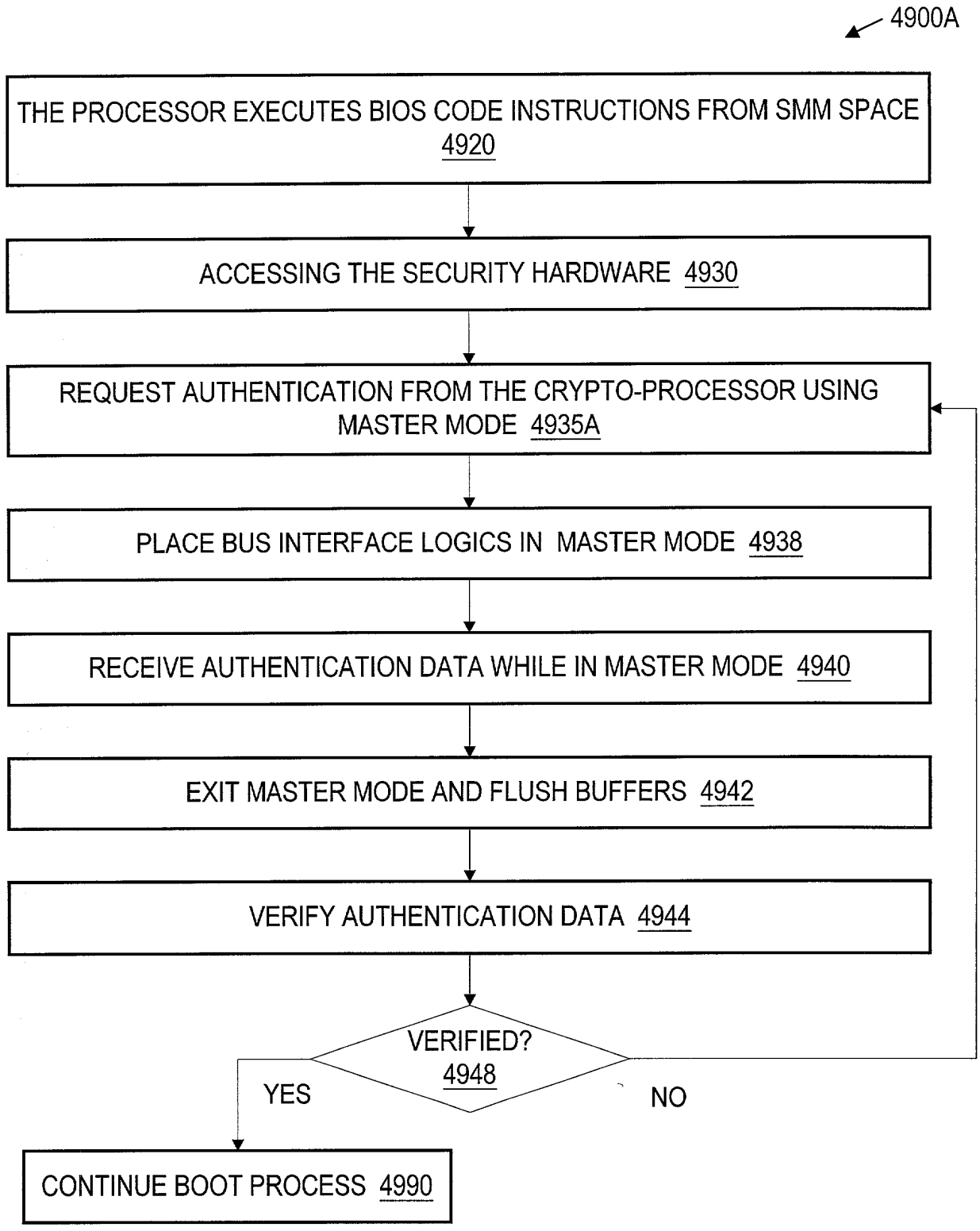

Fig. 38A

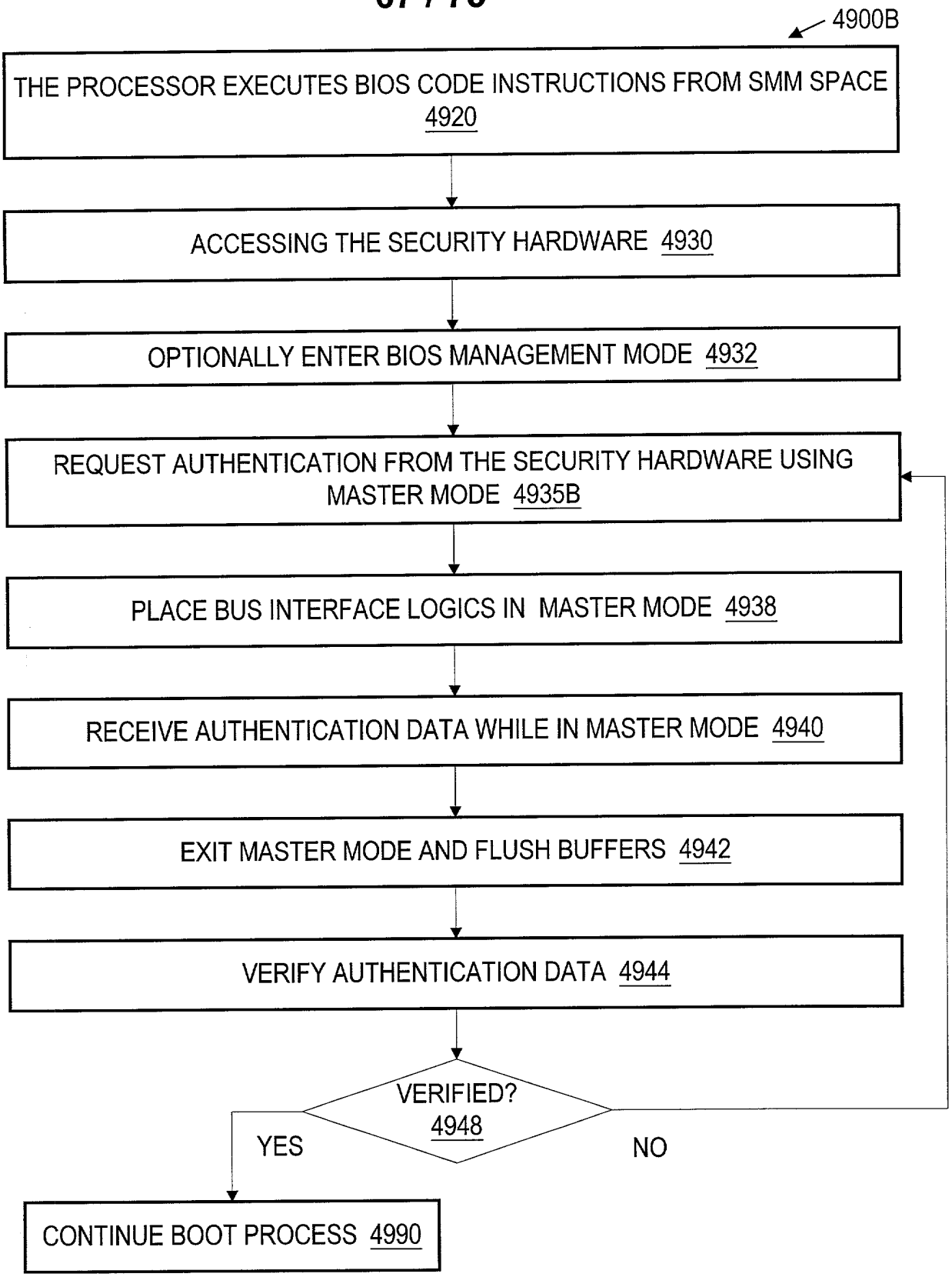
4900B
THE PROCESSOR EXECUTES BIOS CODE INSTRUCTIONS FROM SMM SPACE 4920
ACCESSING THE SECURITY HARDWARE 4930
OPTIONALLY ENTER BIOS MANAGEMENT MODE 4932
REQUEST AUTHENTICATION FROM THE SECURITY HARDWARE USING MASTER MODE 4935B
PLACE BUS INTERFACE LOGICS IN MASTER MODE 4938
RECEIVE AUTHENTICATION DATA WHILE IN MASTER MODE 4940
EXIT MASTER MODE AND FLUSH BUFFERS 4942
VERIFY AUTHENTICATION DATA 4944
VERIFIED? 4948
YES
NO
CONTINUE BOOT PROCESS 4990

Fig. 38B

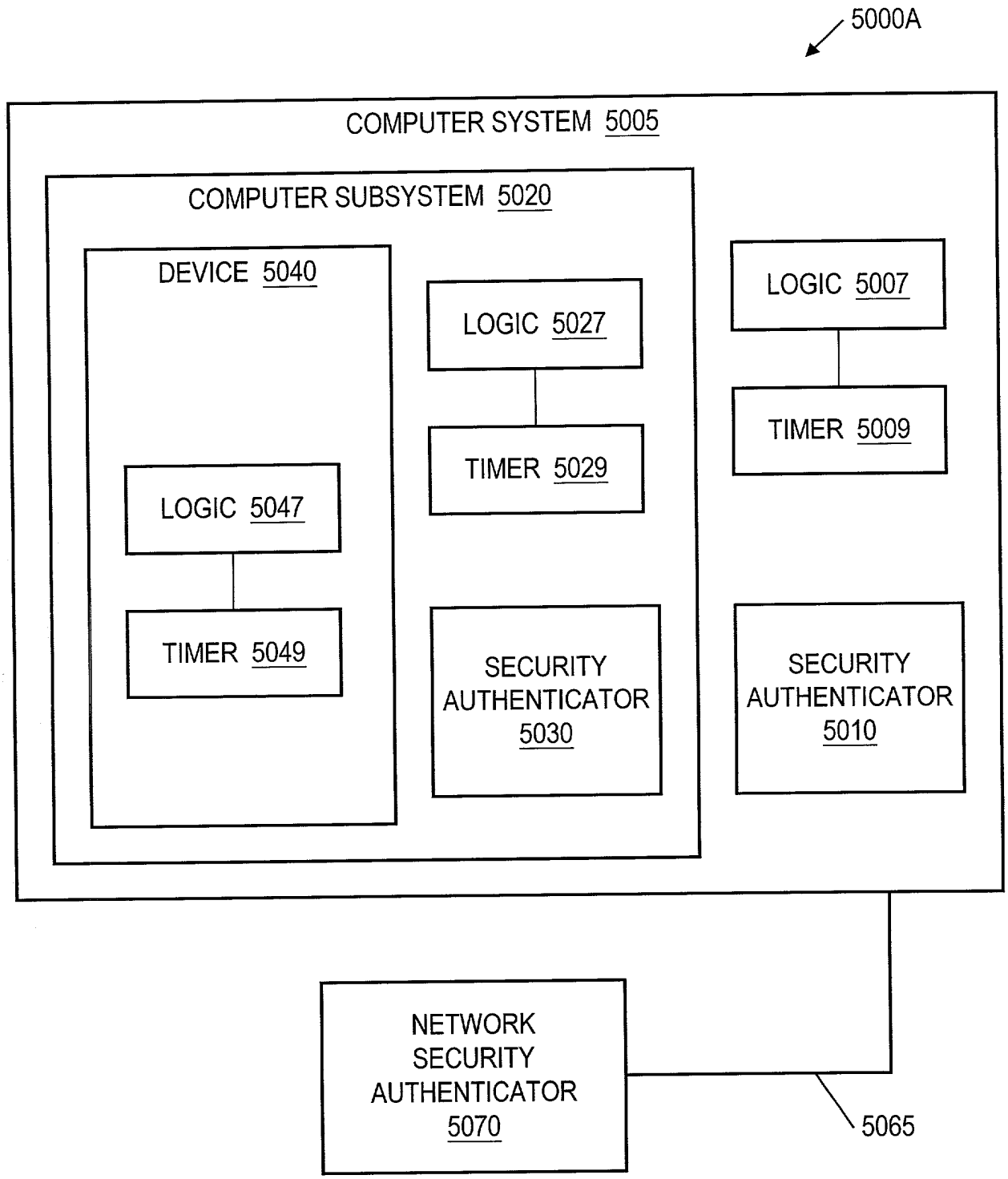

Fig. 39A

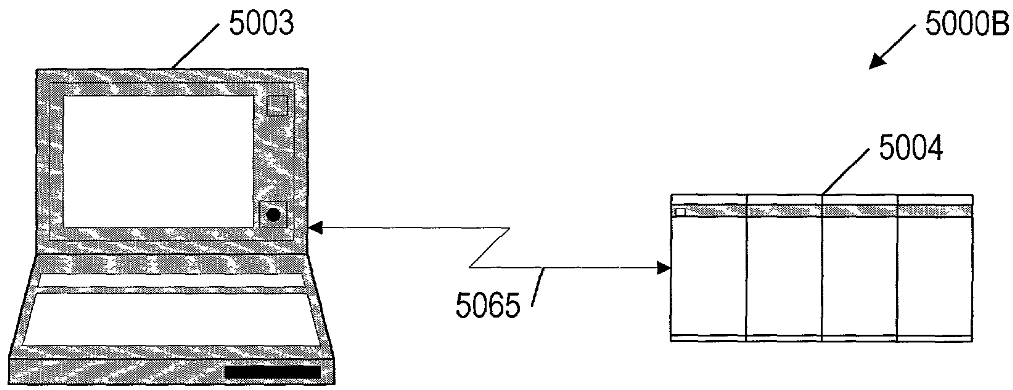

Fig. 39B

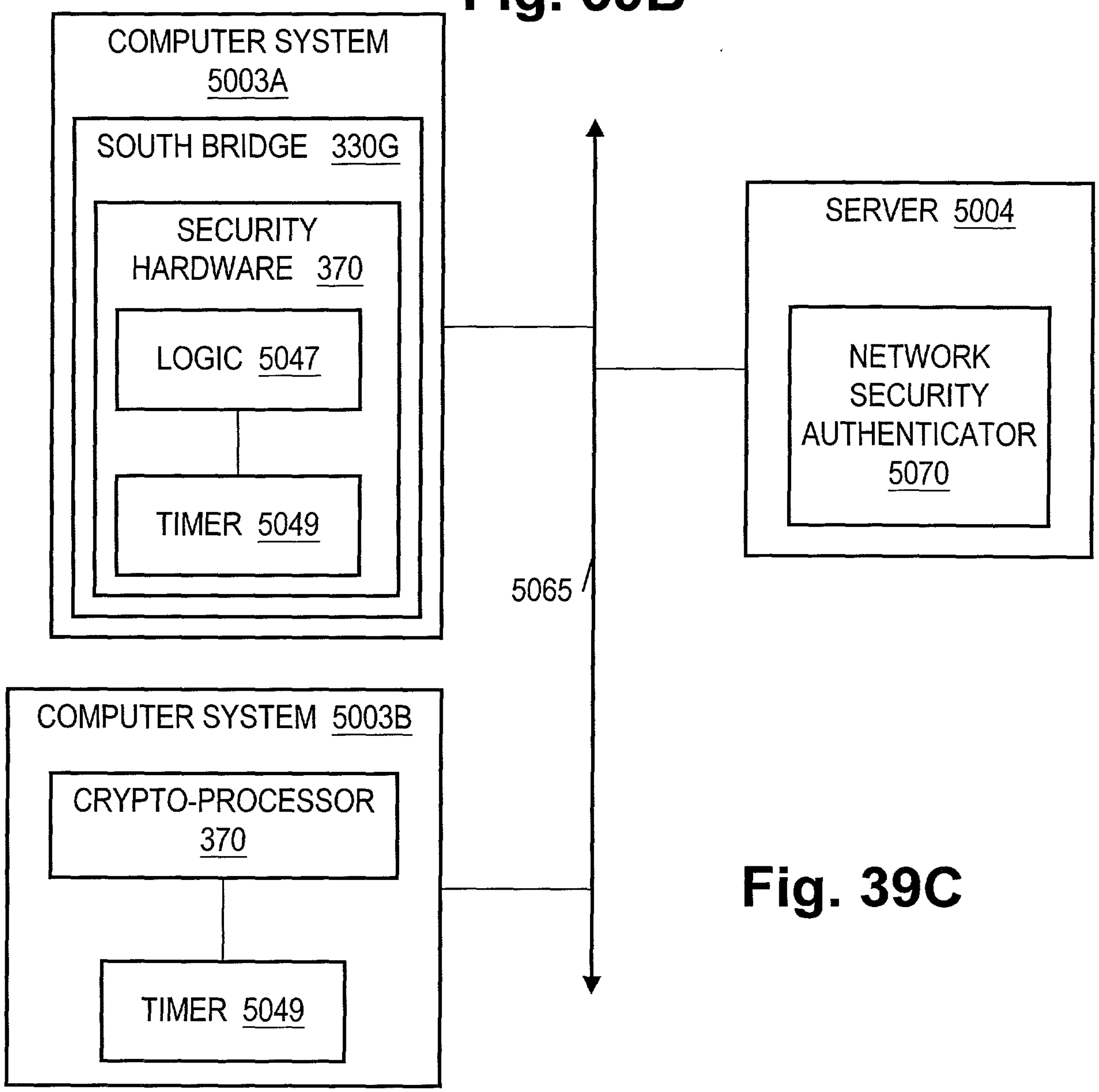

Fig. 39C

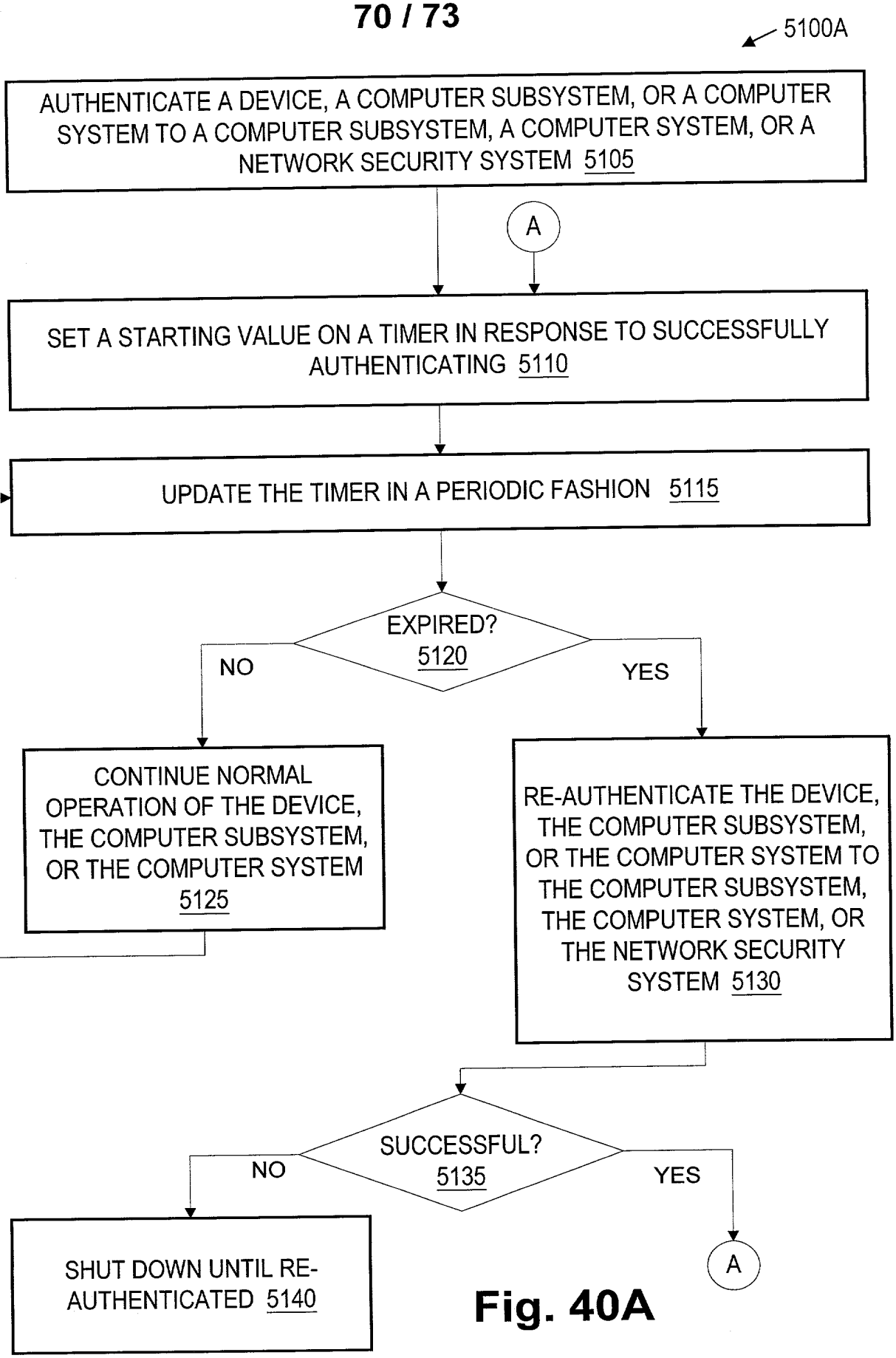

Fig. 40A

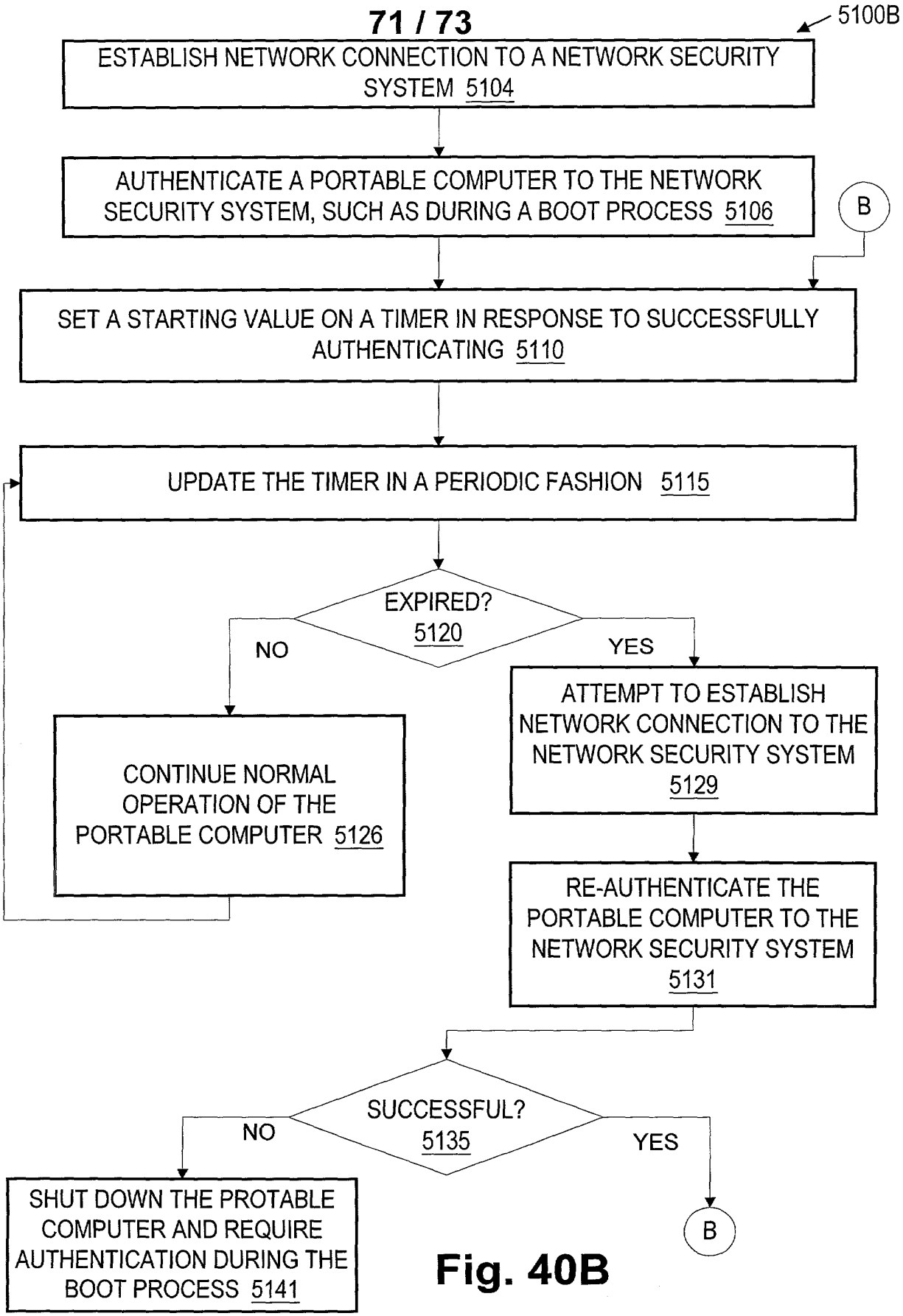

Fig. 40B

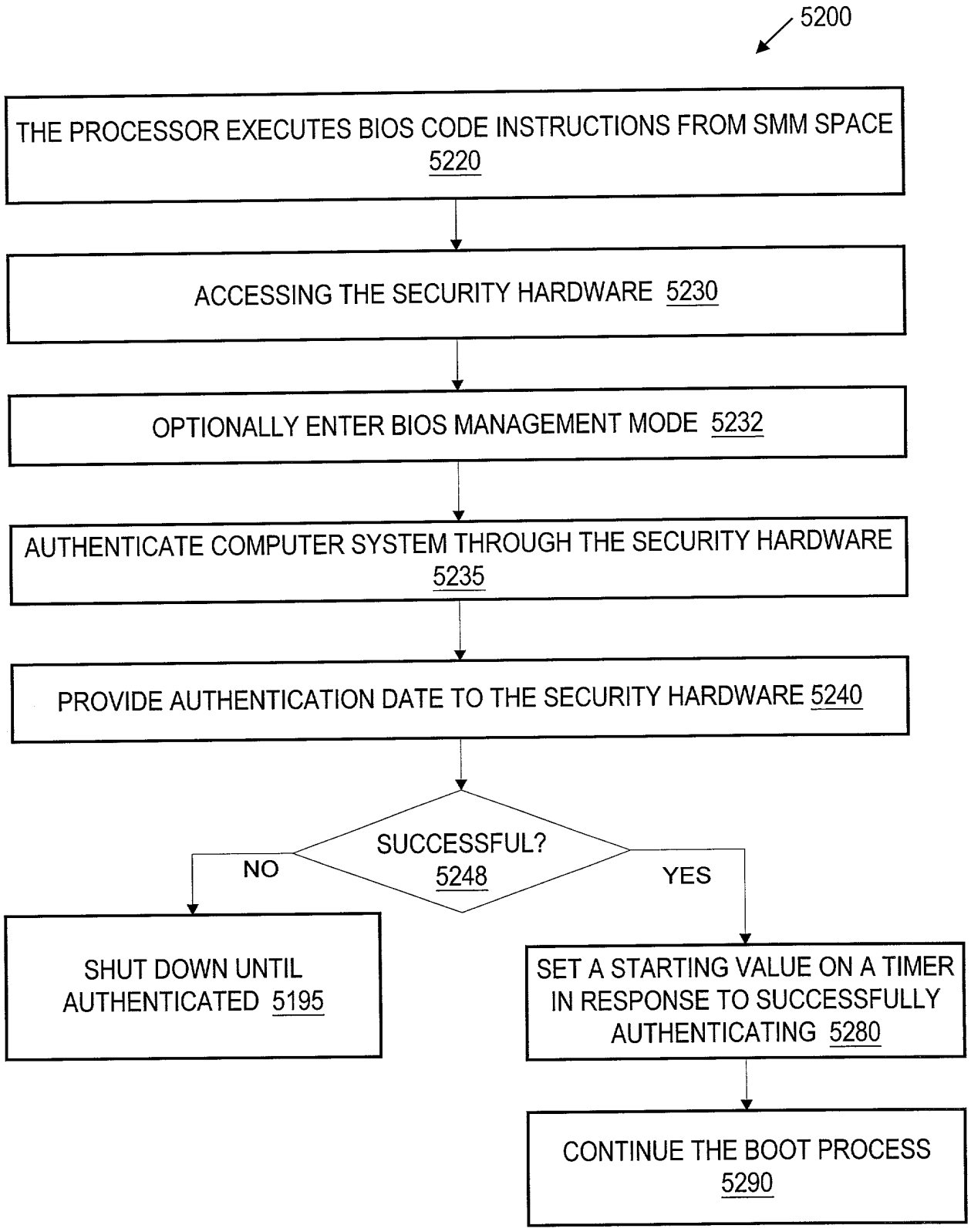

Fig. 41

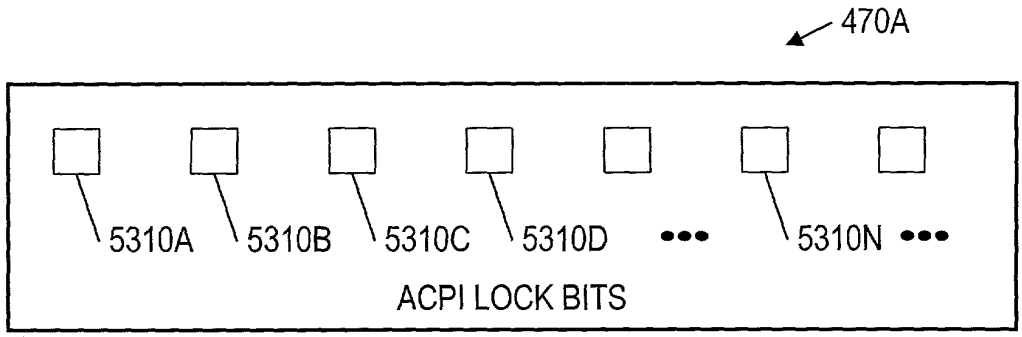

Fig. 42A

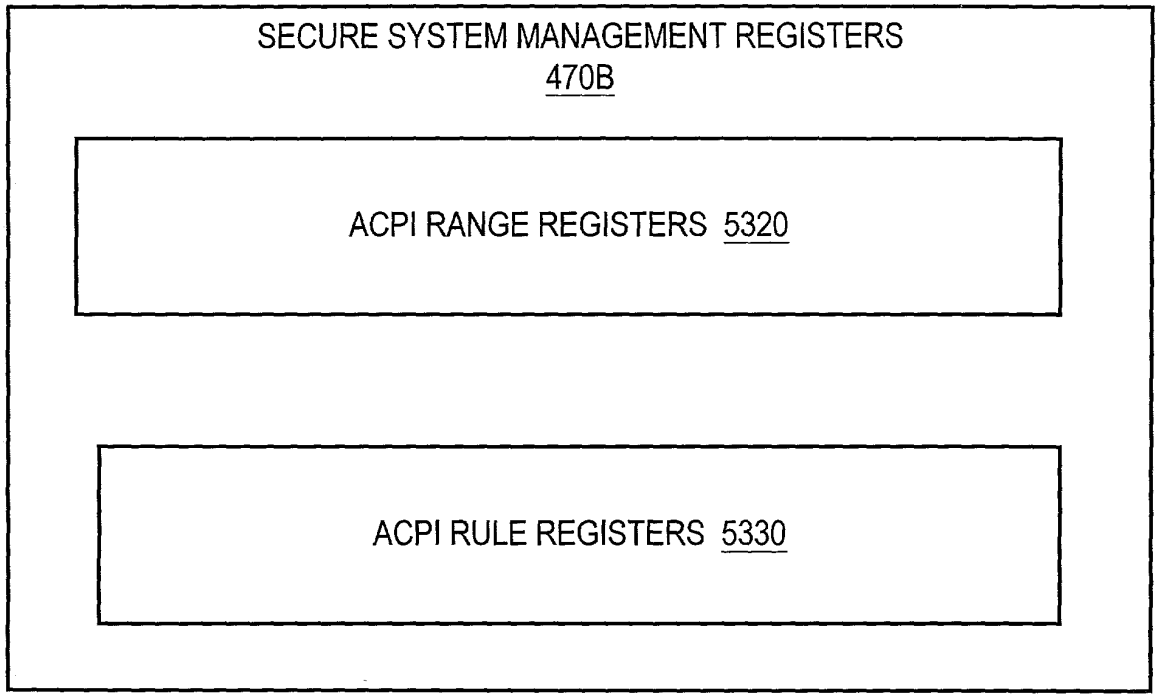

Fig. 42B